UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Actualización de una red local plana a una red local segura, segmentada con servicios de voz y datos en el IFAI

T E S I S

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

OMAR JORGE HERNÁNDEZ JIMÉNEZ

MARCO ANTONIO HUERTA CARMONA

DIRECTORA DE TESIS:

ING. GLORIA GUADALUPE MARTÍNEZ ROSAS

MÉXICO, D.F. Noviembre de 2014

AGRADECIMIENTOS:

Dedicamos estas líneas para expresar nuestros más profundos y sinceros agradecimientos, a todas aquellas personas que con su apoyo físico y moral han hecho posible la culminación de nuestra carrera profesional.

Primeramente agradecer a Dios por sus infinitas bendiciones, amor, brindarnos saludo y fuerzas suficientes para poder llegar hasta el final de nuestras profesión Universitaria, por la gran oportunidad de conocer a muchas personas tan maravillosas y únicas, que han formado parte de nuestras vidas.

A nuestros padres

Omar:	Marco:
Juana Jiménez Guerrero	José Efraín Huerta Hernández
Eladio Hernández Pacheco	María Gloria Carmona Ortega

Quienes ocupan un lugar muy importante en nuestros corazones, quienes nos han heredado el tesoro incondicional más valioso que puede dársele a un hijo, el amor. Sacrificando gran parte de su vida por formarnos y educarnos, jamás podremos pagar todos sus desvelos ni aún con las riquezas más grandes del mundo, por esto y más... gracias.

A nuestros hermanos

Iván Erick Hernández Jiménez	Israel Huerta Carmona
	Erick Alfredo Huerta Carmona
	Gustavo Huerta Carmona

Omar:

A toda el área de la DGTI del IFAI, en especial Andrés Franco, Jorge Virgen, Santiago Covarrubias, Manuel Sánchez... quienes gracias a su apoyo y ayuda fue posible la culminación de este proyecto.

A nuestra directora de tesis, Ing. Gloria Guadalupe Martínez Rosas por su esfuerzo, dedicación y orientación, quien con sus conocimientos, experiencia, paciencia y motivación ha logrado que pudiéramos terminar nuestros estudios con gran éxito.

A nuestros amigos Mariel Martínez Onofre Silvia**,** Pedro Ramírez Cleto, Armando Gómez Bolaños, Edgar Ortiz López, Martín Gómez Jaime… quienes compartimos alegrías y tristezas, amistad, consejos, apoyo, ánimo y compañía. Sin importar en donde estén queremos darles las gracias por formar parte de nosotros.

Marco:
Un agradecimiento muy especial a Mariana Sofía Sánchez Corona, Modesta (aunque ya no está aquí siempre estará en mí recuerdo y corazón) y Agustín, Cinthya Pérez Salomón, Ita Luu Yuyoco Cruz Sherling, Lucero Diana Real Cuautle, Estrella Lorena Real Cuautle, Ocelli Isabel Hernández Lira, Frida Barajas Martínez, Blanca Elena García Gamboa, y mi compañero de tesis Omar Jorge Hernández Jiménez, quienes han formado parte importante de mi vida, gracias a su apoyo y consejos, amistad y compañerismo incondicional, por compartir sus conocimientos e inteligencia; su motivación han hecho posible que siga adelante día con día, así que mi éxito también es suyo… doy gracias a Dios por sus infinitas bendiciones y darme la oportunidad de conocerlos y permitirme disfrutar cada momento y cada instante junto a ustedes, quienes también son mi modelo a seguir.

Sabiendo que nunca existirá una forma de agradecer en esta vida deseamos expresarles que nuestros esfuerzos y logros han sido también suyos, y constituyen el legado más grande que pudiéramos recibir.

Con cariño, admiración y respeto.

ÍNDICE

INTRODUCCIÓN

Hoy en día el buen diseño de una red LAN[1], es uno de los temas fundamentales para la supervivencia de cualquier ambiente de redes de datos, en donde se interconectan dispositivos que a su vez intercambian información, como el de una empresa y/o instituto; las redes de área local actualmente tienden a crecer rápido y constantemente y un mal o escaso diseño dificulta su administración. Un diseño de red el cual no esté dividido en segmentos[2] y además se encuentre en un solo dominio de difusión, puede provocar que una gran cantidad de datos que es transportada por un medio provoque congestionamientos y saturación en la red local.

La red de área local del IFAI, instituto el cual tiene una de red datos plana que brinda servicios a todos sus usuarios locales, demanda diversos recursos, como correo electrónico, telefonía, multimedia, etc. Uno de los principales problemas que el instituto enfrenta, es el aumento excesivo de personal debido a nuevas responsabilidades adquiridas, siendo una de estas la ley de protección de datos. Este tipo cambios ocasionan en la red de área local un agotamiento de direccionamiento IP, aumento del tráfico interno y externo de la red local, que al contar con un mal diseño de red y aunado a tener dispositivos de telecomunicaciones obsoletos, provoque congestionamientos y saturación de la red, brindando servicios deficientes.

El instituto en cuestión al cual se implementará un re-diseño de red, tiene como principal función el resolver la problemática del aumento de personal, la separación de los servicios de voz y datos y la actualización de equipos de comunicaciones, para ello el objetivo de esta tesis, es la incorporación e

[1] **LAN:** de las siglas Local Área Network red de área local es la interconexión de una o varias computadoras.
[2] **Segmento:** parte de una red de computadoras en la que todos los dispositivos se comunican utilizando el mismo medio físico.

implementación de la tecnología VLAN[3], para aislar el tráfico en redes más pequeñas, es decir en subredes[4]; mediante dispositivos como switches y router que ayudarán a facilitar la administración de la red. El proyecto tomará como base una institución con una infraestructura de red plana[5] en la cual se tiene un solo dominio de broadcast[6], se buscará implementar la segmentación por VLAN de los servicios de datos y VoIP[7], con el fin de tener un mejor rendimiento, seguridad y administración de la red, manteniendo la redundancia y la alta disponibilidad, fundamentos necesarios para el óptimo funcionamiento de una red local.

Para cumplir las metas antes mencionadas, esta tesis se divide en: objetivo general, justificación, seis capítulos, conclusiones y fuentes de información. Se planteará el objetivo a alcanzar, por supuesto las justificaciones y las delimitantes del proyecto. En el primer capítulo se describirá el marco teórico y una breve descripción de los antecedentes de las redes, en el segundo capítulo se enfocará en las necesidades, situación actual, ventajas y desventajas que se tendrán con la implementación de una red segmentada sobre una red plana.

En el tercer capítulo se realizará un diseño de la red que satisfaga las necesidades de los usuarios con la implementación de VLAN brindando los servicios de voz y datos. En el cuarto capítulo se presentarán las pruebas realizadas antes de la implementación. En el quinto capítulo se mostrarán todas las configuraciones para obtener una segmentación de los servicios de voz y datos en una nueva red segmentada y en el último capítulo se expondrán los resultados obtenidos, desarrollará documentación del esquema lógico y físico de la nueva red, las

[3]**VLAN:** acrónimo de virtual LAN, red de área local virtual método utilizado para separar una red de varias.
[4]**Subredes:** son redes segmentadas de forma arbitraria por un administrador.
[5]**Red plana**: conjunto de dispositivos conectados entre sí formando un solo dominio de broadcast.
[6]**Broadcast:** dominio de difusión, transmisión de los paquetes que serán recibidos por todos los dispositivos en una red.
[7]**VoIP:** es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP.

contribuciones y mejoras debido a su implementación, oportunidades de mejora, recomendaciones y conclusiones en base a lo implementado.

OBJETIVO GENERAL

La tesis se desarrollará en base a la adquisición de nuevos equipos de telecomunicaciones, con la finalidad de proporcionar a una institución una mejora en su plataforma de servicios de voz y datos actuales, los objetivos principales a cumplir son la seguridad, la escalabilidad, la calidad de servicio, teniendo en cuenta la infraestructura actual y un crecimiento a futuro.

Al término de la tesis se pretende obtener con los equipos de comunicación un mejor control de la administración y seguridad de la red, con la finalidad de proporcionar un servicio integrado de voz y datos, obteniendo así una reducción en los costos, al no instalar los servicios por separado. Para ello se pretende llevar a cabo una topología jerárquica de la red, adquiriendo nuevos equipos con las características necesarias que soportarán las nuevas tecnologías que se utilizarán en este proyecto. Existen tres capas en una topología jerárquica siendo éstas: núcleo, distribución y acceso, cada capa tiene equipos, los cuales cuentan con características que los diferencian de las otras capas.

La capa de núcleo en donde están involucrados los equipos switches core o switches de capa 3, cuya característica primordial es la alta velocidad de procesamiento, esta capa es indispensable para la interconectividad entre los dispositivos de la capa de distribución, los cuales son responsables de la comunicación entre los equipos de la capa de acceso y core, cuya principal función es controlar el flujo de tráfico de la red con el uso de políticas de seguridad y delimita los dominios de difusión a través de las LAN virtuales (VLAN).

Finalmente la capa de acceso, la cual provee la conectividad con los dispositivos finales como PC, impresoras, teléfonos IP, etc., al resto de la red y cuyo propósito es aportar un medio de conexión, además de controlar que equipos podrán comunicarse.

Englobando estos temas y con la implementación de VLAN se pretende satisfacer las necesidades de los usuarios de la red local del instituto, brindando una mayor velocidad en el procesamiento de datos, mejorando la seguridad con la segmentación y creando un dominio de broadcast en cada VLAN, se logrará aislar posibles fallas o problemas a futuro que se podrán identificar y a su vez se reduzca el impacto en toda la red, limitando el problema únicamente al segmento afectado.

JUSTIFICACIÓN

Los beneficios que se pueden obtener al implementar una red de manera jerárquica son:

Escalabilidad, beneficio que se obtiene debido al diseño en módulos, ya que permite introducir los elementos de capa conforme crece la red, facilitando la planificación e implementación de una posible expansión.

Redundancia, en una red que crece constantemente la disponibilidad toma un factor importante, ya que en una red jerárquica el agregar enlaces redundantes, proporcionan una ruta disponible tanto en la capa de distribución como en la de núcleo, no así en la capa de acceso que por restricciones de los mismos equipos, no es posible conectar un dispositivo final a más de un switch.

Rendimiento, beneficio que se obtiene al garantizar que las capas de núcleo y distribución realicen sus comunicaciones a altas velocidades y que en la capa de acceso se mantenga en lo posible un puerto por usuario.

Seguridad, aspecto que se mejora aplicando políticas en la capa de distribución haciendo que la red sea menos susceptible a accesos no permitidos, aunado a

todo esto se suma la facilidad de administración, una vez que se logra alcanzando una consistencia en cada capa, hace que la administración sea más simple y fácil, la modularidad de este modelo jerárquico permite que la red escale sin volverse demasiado complicada.

Para la implementación de la nueva estructura de red, es decir, la migración de una red plana a una red segmentada se necesita evaluar el funcionamiento actual, definir los roles que se tendrán tanto los usuarios como los administradores, además, ver la proyección a futuro del personal, cuales son los problemas actuales, las herramientas con las que cuenta la institución tales como IDS[8], IPS[9], firewalls[10], así como la segmentación que es utilizada; todo esto para tener en cuenta qué segmentos son necesarios y cuáles se podrán utilizar para los usuarios, administradores e interfaces de administración de los equipos, dado que éstos deben ser diferentes por cuestiones de seguridad y buenas prácticas.

Otro tema importante que se debe tomar en cuenta es la antigüedad de los equipos, ya que como se mencionó, se desea migrar la red y por ello se deberá tomar la decisión, si los equipos actuales podrán soportar la implementación de una red de voz y datos, por esta razón uno de los primeros asuntos a tratar fue la elección del nuevo Hardware, que cumpliera con los servicios tanto en el aspecto de datos como de voz.

Por tal motivo, para la implementación de los nuevos segmentos de red que operarán con la tecnología VLAN, se deberá analizar el actual diseño de la red LAN, para así adecuar los cambios en base a las capas de la topología de la red

[8] **IDS:** de las siglas Intrusion Detection System, sistema de detección de intrusos es un programa usado para detectar accesos no autorizados a un computador o a una red.
[9] **IPS:** de las siglas Intrusion Prevention System, sistema de prevención de intrusos es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
[10] **Firewall:** cortafuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

jerárquica y así lograr un mejor control de la red LAN[11], ya que las VLAN proporcionan segmentación, flexibilidad y seguridad. Teniendo en cuenta que se tiene una red plana, en la cual hay una segmentación para la red de usuarios, una para aplicaciones, otra más para bases de datos y una última red Ethernet aislada, la cual estará abierta al público.

El aspecto en el cual se centra la atención del actual diseño de la red y es el más importante de acuerdo a la topología en estrella, siendo este el firewall quien controla y restringe estos segmentos, la solución que se plantea es la segmentación para el servicio de datos en la red de usuarios a través de la implementación de VLAN por piso, en un ambiente alámbrico y la segmentación de una VLAN dedicada al servicio de voz, ofreciendo así, una mejor distribución del tráfico en la red y la modulación de servicios para tener identificados que servicio está conectado en que puerto de cada switch, todo ello cuidando los aspectos de alta disponibilidad y redundancia vigentes en la red actual.

En el análisis de la segmentación de VLAN para el centro de datos(MDF[12]) se realizó considerando los ambientes de producción, desarrollo, bases de datos y usuarios, con la finalidad de obtener un mejor control de cada uno de los ambientes, para el caso de la segmentación de los pisos se analizó la posibilidad de dividirlos por área administrativa o por piso, dado que en el instituto el personal se encuentra distribuido de manera desordenada y es difícil reorganizarlos, se tomó la propuesta de las VLAN[13] por piso otorgando hasta 2046 direcciones IP[14] previendo un crecimiento del personal con el direccionamiento IP 172.19.X.X/16.

[11] **LAN:** de las siglas Local Área Network red de área local es la interconexión de una o varias computadoras
[12] **MDF:** Main Distribution Frame
[13] **VLAN:**Acrónimo de virtual LAN, red de área local virtual y su protocolo de utilización es el IEE 802. IQ.
[14] **IP:** es un protocolo de comunicación de nivel 3 de la capa OSI.

Para el direccionamiento IP de los servidores, se propuso el segmento 172.20.X.X/24 permitiendo asignar hasta 254 direcciones IP por segmento, ya que es más que suficiente el número de direcciones IP propuesta para tener una segmentación ordenada, un punto que se consideró fue la administración de los equipos de telecomunicaciones (firewalls, balanceadores, los switches core, de distribución y de acceso) para ello se consideró el segmento de red 172.16.37.X/30, 10.1.1.0/24 y 172.17.29.X/30.

El servicio de VoIP, será un servicio nuevo implementado que debido al nuevo esquema de red propuesto, permite la protección del segmento de voz contra alguna falla, incidente o problema que se pudiese presentar en los segmentos de red de datos y al pertenecer a una VLAN diferente se garantiza la disponibilidad del servicio, para el direccionamiento del servicio de telefonía se propone un segmento de red 172.18.0.X/21 permitiendo asignar hasta 2046 direcciones IP a los usuarios de telefonía VoIP del instituto, se consideró esto ya que el número de usuarios del instituto actualmente es de 500 y con este nuevo direccionamiento se satisfacerá esta necesidad, además de que permite un crecimiento a futuro.

Con el fin de estar en la mejora continua se planeó un cambio en varios aspectos en la red, se comenzó por la migración de los equipos de telecomunicaciones a equipos con mayor capacidad de procesamiento, para ello se realizó un análisis de lo que actualmente se encuentra conectado y cuáles serían las mejores acciones para reorganizar el esquema de la red, por lo cual se planteó una propuesta de segmentos (módulos) de usuarios internos, bases de datos, aplicaciones, QA, desarrollo y respaldos.

Algunos de los beneficios al implementar VLAN son:

- Mayor flexibilidad en la administración y en los cambios de la red.
- Proporcionan mayor seguridad, ya que si algún usuario se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuración cierta cantidad de puertos para cada VLAN.
- Controla la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.
- Una red sin VLAN se considera plana, donde el broadcast se repite en los puertos provocando una situación crítica. Con las VLAN existe una segmentación lógica o virtual.

DELIMITACIONES

Para el proyecto en particular sólo se tomarán los servicios de voz y datos en un ambiente alámbrico y con una red plana, sin entrar en detalles de instalación y configuración de telefonía como conmutador, tarificador, enlaces troncales, etc., que son indispensable para el funcionamiento de la telefonía, pero sólo se verá como un servicio que será implementado en una sola plataforma, tampoco se mencionará el tema de red inalámbrica que cabe mencionar es importante, pero debido que la seguridad es un tema demasiado extenso, pudiendo ser tema de otro proyecto de tesis. Tratar de implementar una red inalámbrica sin contar con una seguridad robusta, sería un riesgo, sin mencionar que presentaría una contradicción con los principios antes mencionados.

Otra limitante es la manera como se otorgarán las direcciones IP, que para este proyecto no se entrará en detalles, ya que hablar de ello ampliaría demasiado el tema, porque se tendría que hablar si se asignarán las direcciones IP de manera estática o de forma automática, esto último con un servicio de DHCP, que a su vez deberá contar con redundancia y alta disponibilidad, tampoco se tomará en cuenta la seguridad, que es un tema de alta importancia y no se debería dejar de lado, para ello se mencionará una alternativa de cómo solucionar este tema, aunque no se verá la instalación y configuración de dicha solución.

CAPÍTULO I
MARCO TEÓRICO

CAPÍTULO I. MARCO TEÓRICO

1.1 ANTECEDENTES

La historia de cómo iniciaron los primeros equipos de cómputo para formar una interconexión entre ellos y los dispositivos[15], es muy extensa, por lo tanto sólo se hace referencia a los acontecimientos más relevantes.

1.1.1 PRIMERA GENERACIÓN

Estas máquinas estaban construidas por medio de tubos de vacío. Los equipos de cómputo eran de gran tamaño y consumían una gran cantidad de electricidad provocando un desprendimiento excesivo de energía calorífica lo que propiciaban fallas. La primera computadora electrónica ENIAC (Electronic Numerical Integrator And Calculator) construida en 1947 en la Universidad de Pennsylvania, tenía la capacidad de realizar 5,000 operaciones aritméticas en un segundo, pero ocupaba todo un sótano de la Universidad equivalente a una salón de baile y requería todo un sistema de aire acondicionado.

En 1951 aparece la UNIVAC (UNIVersal Automatic Computer), primera computadora comercial, que disponía de mil 1024 bytes de memoria central y podían leer cintas magnéticas.

1.1.2 SEGUNDA GENERACIÓN

La característica de la segunda generación era que los equipos estaban construidos con circuitos de transistores. Estas computadoras se programaban con cintas perforadas y otras por medio de cableado en un tablero, los programas eran hechos a la medida por un equipo de expertos. Las computadoras de esta generación fueron: la Philco 212 (esta compañía se retiró del mercado en 1964) y la UNIVAC M460. La Radio Corporation of America introdujo el modelo 501 que

[15] **Dispositivo:** es una estación emisora de una trasmisión, es decir cualquier sistema conectado a la red.

manejaba el lenguaje COBOL[16], para procesos administrativos y comerciales; cada vez se daba un gran salto en la tecnología.

1.1.3 TERCERA GENERACIÓN

En 1960 se inventó el circuito integrado con muchos transistores en un pequeño semiconductor. La fabricación electrónica de estos equipos estaba basada en circuitos integrados y su operación era por medio de lenguajes de control de los sistemas operativos[17]. A mediados de la década de 1970, aparecieron en el mercado las computadoras de tamaño mediano denominados minicomputadoras, aunque realmente su tamaño era grande si se compara con los actuales.

1.1.4 CUARTA GENERACIÓN

Aparecen los microprocesadores, circuitos integrados de alta densidad y con una alta velocidad de procesamiento. Esto permitió la creación de las microcomputadoras con Apple Computer Company que presentaría en 1977 la primera computadora personal; cuatro años después IBM (International Business Machines Corporation) también expuso su primer equipo personal, como resultado de ambos se dio la difusión de computadoras hasta los hogares.

En la década de 1980 los equipos de cómputo ya empezaban a utilizar módems[18] a las que se denominaron comunicaciones de punto a punto o de acceso telefónico, esto dio origen al uso de dispositivos que funcionaban como punto central de comunicación en una conexión de acceso telefónico, llamados tableros de boletín.

[16] **CO**mmon **B**usiness-**O**riented **L**anguage

[17] **Sistema Operativo:** Software que realiza tareas básicas tales como controlar y asignar memoria, priorizar pedidos de sistema, controlar dispositivos de entrada y salida.

[18] **Módem:** dispositivo que convierte las señales digitales en señales analógicas que pueden transmitirse a través del canal telefónico.

Este tipo de sistema tenía dos inconvenientes, la primera que existía poca comunicación directa y sólo permitía la interacción de los usuarios conectados al mismo tablero de boletín, y la otra, era necesario un modem por cada usuario, si una gran cantidad se conectaba simultáneamente era necesario la misma cantidad de módem y líneas telefónicas, por lo tanto esto no era factible ni conveniente por la alta demanda.

La primera versión original de red de área local del mundo fue diseñada por Robert Metcalfe denominada Ethernet, pretendía que fuera un estándar compartido y que todos se pudieran beneficiar, lo que implicó que se distribuyera como un estándar abierto. A principios de la década de 1980 se vendieron los primeros productos desarrollados para Ethernet[19].

1.1.5 QUINTA GENERACIÓN

Japón lanzó en 1983 el llamado "programa de la quinta generación de computadoras" que tenía como objetivo el procesamiento en paralelo mediante arquitecturas, circuitos de gran velocidad, manejo de lenguaje natural y sistemas de inteligencia artificial. En realidad la idea es crear una máquina que pudiera comportarse como un ser humano que piense y razone, sin embargo, recientemente es cuando se empieza a ver algunos productos como identificar el rostro de una persona, leer un texto, entender una conversación, hablar, entender órdenes, aunque se ha visto avances nunca imaginados, aún falta mucho camino por recorrer.

[19]**Ethernet:** especificación de LAN de banda base inventada Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation.

1.2 MODELO OSI

Para enfrentar el problema de incompatibilidad de Software y Hardware se establece el modelo OSI (Open System Interconnection) programa de estandarización creado por la ISO[20] y la UIT-T[21] para desarrollar estándares de interconexión que facilite la interoperabilidad de equipos de distintos fabricantes.

El modelo OSI (Fig. 1) está conformada por siete capas lógicas creada como guía para el diseño del protocolo de red, cada capa tiene una única funcionalidad con protocolos[22] y servicios asignados específicamente.

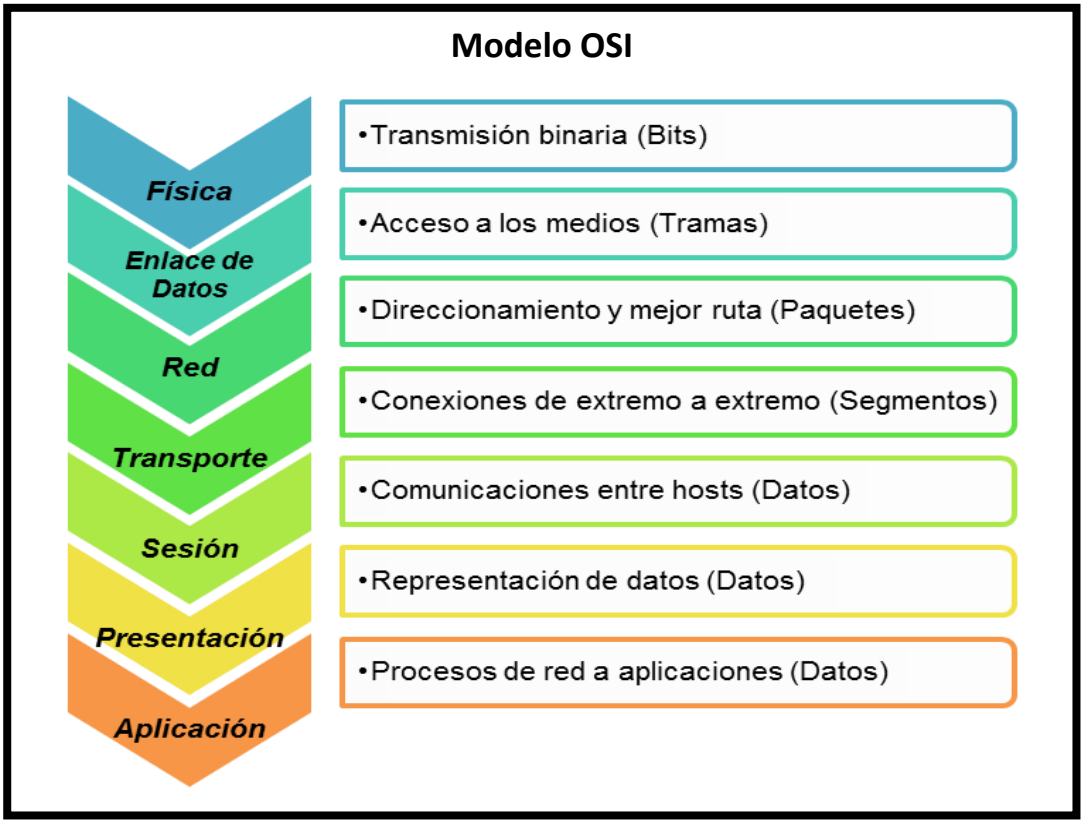

Fig. 1 "Modelo OSI" Fuente:*CCNA Exploration 4.0, Módulo I, Aspectos básico de networking.*

[20]**ISO:**International Organization for Standardization

[21]**UIT-T:**Sector de Normalización de las Telecomunicaciones (antes CCITT).

[22]**Protocolos:** conjunto de reglas que rigen la comunicación.

Las diferentes funciones de cada una de las capas del modelo OSI y del protocolo TCP/IP[23] logran de manera eficiente y efectiva la comunicación. El buen análisis es clave en los protocolos TCP y UDP[24] que son base para el funcionamiento desde la red más pequeña hasta la red más grande, dado que la Internet se creó utilizando dichos protocolos.

La comunicación entre los equipos de una red requiere, la interacción de un gran conjunto de protocolos interrelacionados, denominado suite de protocolos, implementados en el Software y Hardware de cada dispositivo de la red. El modelo de interconexión OSI es el modelo de red más conocido, para el diseño de las redes de datos.

Una de las capas con la que los usuarios tienen relación es la última capa del modelo OSI y TCP/IP que corresponde a la capa de aplicación, encargada de proporcionar la interfaz de las aplicaciones para la comunicación entre usuarios y la red adyacente en la cual se trasmiten los mensajes.

1. Capa física: En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación.

2. Capa de enlace de datos: La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación, que al llegar a la capa de red aparezca libre de errores de transmisión

3. Capa de red: Determina el mejor camino, utilizando direccionamiento lógico (IP).

[23]**TCP/IP:** Protocolo de Control de Transmisión /Protocolo de Internet. Nombre común para el conjunto de protocolos desarrollado por el DoD (Department of Defense) de EE.UU. en la década de 1970 para permitir la creación de redes interconectadas a nivel mundial.

[24]**UDP:**User Datagram Protocol es un protocolo simple que intercambia datagramas sin acuses de recibo ni garantiza el envío, que requiere que el procesamiento de errores y la retransmisión sean administrados por otros protocolos.

4. Capa de transporte: La función básica de esta capa es aceptar los datos provenientes de las capas superiores, re ensambla los segmentos que llegan en desorden, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo.

5. Capa de sesión: Esta capa permite que los usuarios de máquinas diferentes establezcan, manejen y terminen sesiones entre ellos.

6. Capa de presentación: A esta capa le corresponde la sintaxis y la semántica de la información transmitida, es decir, facilita el trabajo de las entidades de la capa de aplicación traduciendo varios formatos de datos.

7. Capa de aplicación: Brinda los servicios de comunicación a los usuarios, protocolos y Software al servicio del usuario (Navegadores Web, correo electrónico, etc.).

En la siguiente (Fig. 2) se observan los protocolos que interactúan en cada una de las capas del Modelo OSI hasta llegar a la última (aplicación) donde el usuario final interactúa.

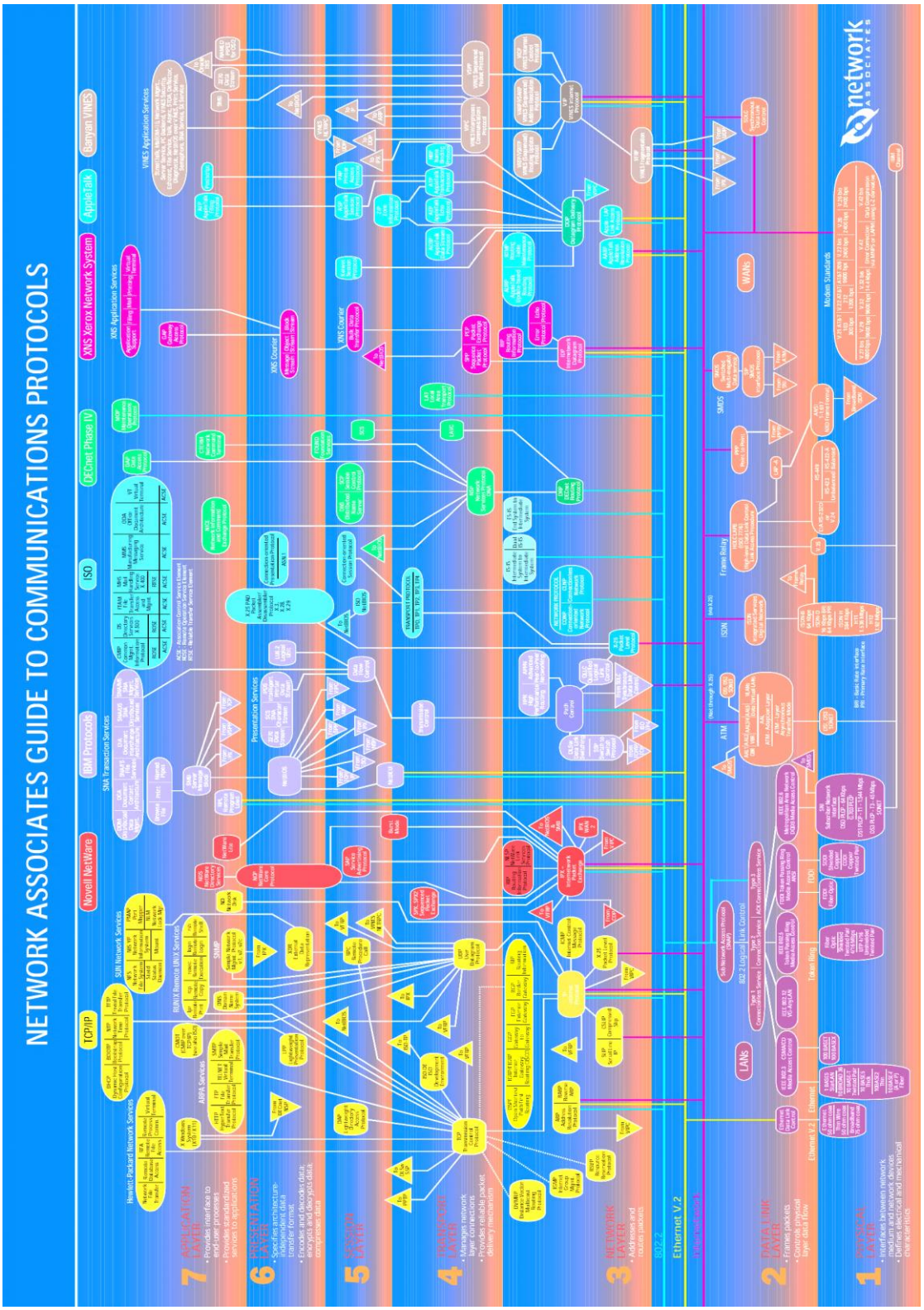

Fig. 2 “Protocolos de Comunicaciones”
Fuente:http://sebsauvage.net/comprendre/tcpip/protocols.pdf

1.2.1 REDES LAN

Las LAN es el acrónimo Local Area Network, el Institute of Electrical and Electronics Enginners define la red local como un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre sí. Las redes de área local aparecieron a finales de la década de 1970 por la necesidad de compartir datos y servicios entre usuarios de una misma área de trabajo.

El estándar IEEE 802.3 aparece gracias al protocolo de Ethernet propuesto por las empresas Xerox, Intel y Digital Equipment Coporation, en el año de 1970 el protocolo que predominaba era el Token ring de IBM. El estándar está diseñado para poder ser implementado en distintos medios físicos con distintas velocidades de trasmisión.

Las redes de datos aparecieron como consecuencia de la necesidad de compartir e intercambiar información en la actividad comercial, en un principio los equipos de cómputo no estaban conectados entre sí, por lo que no había una manera eficaz ni económica de compartir datos entre varios equipos de cómputo. La manera de hacerlo era por medio de disquetes, que no era el método apropiado, porque se tenían que crear copias para cada usuario para que la información llegara lo más rápido posible a su destino y cada vez que se modificaba un archivo había que volver a compartirlo.

En consecuencia, surgieron dos grandes problemas que necesitaban pronta solución:

- Comunicación con eficiencia.
- Configuración y administración de la red.

No paso mucho tiempo para darse cuenta que las redes de computadoras podían aumentar la productividad y ahorrar gastos innecesarios, aunque en la década de 1980 su desarrollo era desorganizado esto no impidió que su expansión fuera de gran importancia. Esta tecnología tenía un inconveniente, que se había creado con distintos estándares, cada empresa desarrollaba sus propias aplicaciones de Software y Hardware, por lo tanto no eran compatibles entre sí.

Cada vez se tornaba más difícil la comunicación entre las redes que utilizaban sus propias implementaciones corporativas, la solución fue la creación de los estándares que hizo posible la estabilidad y compatibilidad de los equipos.

1.2.2 CARACTERÍSTICAS DE LAS REDES LAN

Actualmente las redes de área local constan de lo siguiente:

- ***Computadora***: Máquina que recibe y procesa datos para convertirlos en información útil.
- ***Periférico***: Dispositivo electrónico físico que se conecta o acopla a una computadora.
- ***Medios de red***: Los diversos entornos físicos a través de los cuales pasan las señales de transmisión (par trenzado, cable coaxial, fibra óptica y la atmósfera).
- ***Dispositivos de red***: Extremo final de una conexión de red o unión común a dos o más líneas de una red.
- ***Tarjeta de interfaz de red***: Placa que suministra capacidades de comunicación de red hacia el sistema informático y desde éste.

Los cuatro elementos que conforman una red son:

- ***Reglas***: Permite generar restricciones a los host disminuyendo vulnerabilidades.
- ***Medio***: Son los diversos entornos físicos a través de los cuales pasan las señales de transmisión.

- ***Mensajes***: Agrupaciones lógicas de información de la capa de aplicación.
- ***Dispositivos***: Extremo final de una conexión de red.

Tecnologías de red de área local:

- ***Ethernet***: Especificación de LAN de banda base inventada por Xerox Corporation y desarrollada de forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet usan CSMA/CD[25] y se ejecutan a través de varios tipos de cable a 10 Mbps. Ethernet es similar al conjunto de estándares IEEE 802.3.
- ***Token ring***: LAN de entrega de token desarrollada y apoyada por IBM. Las token ring operan a 4 ó 16 Mbps mediante una topología de anillo. Similar a IEEE 802.5.
- ***FDDI***: (Fiber Distributed Data Interface) Estándar LAN, definido en ANSI X3T9.5, que especifica una red de transmisión de token de 100 Mbps que usa cable de fibra óptica, con distancia de hasta 2 Km. FDDI usa una arquitectura de anillo doble para proporcionar redundancia.
- ***Fibra óptica***: Medio físico que puede conducir una transmisión de luz modulada.

Las LAN están diseñadas para:

- Operar dentro de un área geográfica ilimitada.
- Múltiples accesos a medios con alto ancho de banda.
- Controlar la red de forma privada con administración local.
- Conectividad continúa a los servicios locales.
- Conectar dispositivos físicamente adyacentes.

[25]**CSMA/CD:** mecanismo de acceso a los medios en que los dispositivos que están listos para transmitir datos verifican primero el canal en busca de una portadora. Si no se detecta ninguna portadora durante un período de tiempo determinado, el dispositivo puede comenzar a transmitir. Si dos dispositivos transmiten al mismo tiempo, se produce una colisión.

1.2.3 DISPOSITIVOS EN LAS LAN

- ***Hub**:* Dispositivo que recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.
- ***Router**:* Dispositivo de capa de red, que usa una o más métricas para determinar la ruta más corta a través de la cual se debe enviar el tráfico de la red.
- ***Puente**:* Dispositivo de capa 2, que conecta múltiples segmentos de red en la capa enlace de datos del modelo OSI.
- ***Repetidor**:* Dispositivos que regenera y propaga señales eléctricas entre dos segmentos de red.
- ***Switch**:* Dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama.

Factores al seleccionar un dispositivo para una LAN

- Costo.
- Velocidad, tipos de puertos e interfaces.
- Posibilidad de expansión.
- Administración.
- Características y servicios adicionales.

1.3 ARQUITECTURA DE UNA RED

Hoy en día para toda institución y empresa, la comunicación digital de datos y voz es esencial para su éxito, por esa razón es fundamental la selección apropiada en el diseño de la red LAN y contar los dispositivos adecuados. La buena selección de la arquitectura da como beneficio, que la red se administra y expanda con más facilidad y los problemas que pudieran surgir, se habrán de resolver con mayor rapidez.

Las redes deben funcionar con diferentes tipos de arquitecturas, como también admitir una extensa variedad de servicios y aplicaciones, además, debe ser redundante para permitir rutas alternas, para lograr que el usuario no vea afectado el servicio utilizado, en dado caso que algún dispositivo redundante o enlace pudiese llegar a fallar.

1.3.1 TIPOS DE TOPOLOGÍAS DE UNA RED

La estructura de una red es definida por la topología de red, que a su vez está constituida en dos partes, la primera compuesta por la topología física referente a la configuración de cables, computadoras y otros periféricos, donde se diferencian dos tipos de conexiones: punto a punto y multipunto.

La segunda parte es la topología lógica, que define la forma en que los host acceden a los medios para enviar datos, es decir, el trayecto de las señales y la comunicación entre ellos, además, muestra el flujo de datos en una red; por lo tanto la topología tiene como objetivo establecer un orden de conexión y comunicación de los recursos de la red de la manera más eficiente y eficaz, para evitar conflictos si nuevos dispositivos son colocados de forma aleatoria y satisfacer la demanda de los usuarios con un tiempo de espera lo más reducido posible.

Las topologías físicas más comunes son:

- Topología de bus.
- Topología en estrella.
- Topología de anillo.
- Topología de árbol.
- Topología en malla.

1.3.2 TOPOLOGÍA BUS

Es la topología más sencilla, todos los host están conectados directamente a un canal de comunicación denominado bus o backbone (Fig. 3) en cada extremo del cable debe existir un terminador para evitar que las señales nuevamente regresen a los equipos conectados al bus, la gran desventaja de la topología es que la información que se envía por el medio de comunicación llega a todos los host conectados, lo que hace posible que cada host acceda a los datos trasmitidos.

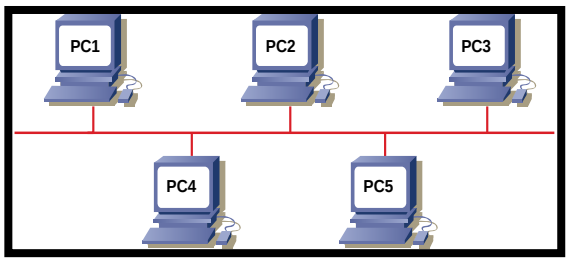

Fig. 3 “Topología Bus” Fuente:*Tecnologías y redes de transmisión de datos, Enrique Herrera Pérez.*

Cada equipo tendrá que comparar la dirección de destino de los datos para verificar si la información recibida es para él, de lo contrario es descartado.

Ventajas

- Su instalación es fácil por la sencillez de su topología.
- Añadir o eliminar un host es sencillo.
- No es necesario que todos los equipos estén activos para el buen funcionamiento de la red.

Desventajas

- Al estar conectados todos los equipos a un mismo medio se producen problemas de tráfico y colisiones.
- No se tiene redundancia, si el bus se rompe quedan todos los host incomunicados.
- La resolución de errores puede resultar difícil.

1.3.3 TOPOLOGÍA ESTRELLA

Existe un nodo central que puede ser un switch o un hub enlazado con todos los equipos, quien controla todo el tráfico de la red reenviando los datos a su destino. Cada nodo tiene un enlace punto a punto con el nodo central, su funcionamiento es fácil de entender si un host quiere enviar información a otro, primero llega al nodo central quien posteriormente los reenvía a un nodo en particular (destino) o a todos, esto dependerá si es un Switch o hub (Fig. 4).

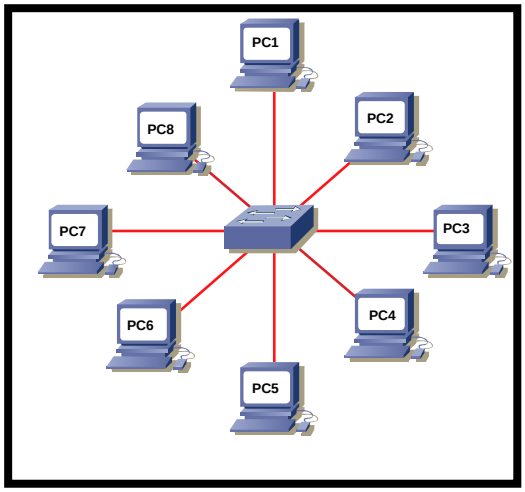

Fig. 4 "Topología Estrella" Fuente:*Tecnologías y redes de transmisión de datos, Enrique Herrera Pérez.*

Ventajas

- Diseño simple, fácil de instalar y mantener.
- Su funcionamiento no depende de los host, si tiene alguna falla la red, ésta sigue funcionando.
- Resolución de fallas y detección de las mismas es sencillo.

Desventaja

- Si el nodo central falla la red no funciona.
- Todo el tráfico pasa por el nodo central lo que provoca un cuello de botella.

1.3.4 TOPOLOGÍA ANILLO

Cada equipo está conectado con dos nodos adyacentes formando un círculo o un anillo cerrado, por el cual viajan los datos, los enlaces son de punto a punto, donde la información va pasando por los host intermedios hasta llegar a su destino y siempre en el mismo orden, cerrando el anillo con la primera y última estación (Fig. 5).

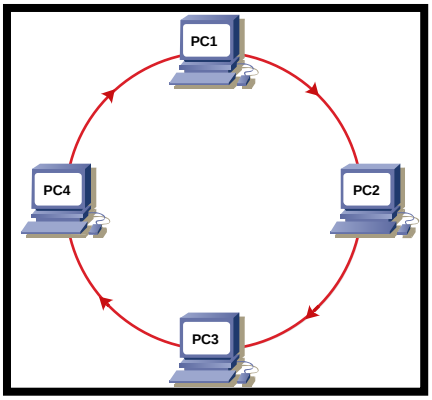

Fig. 5 "Topología Anillo" Fuente:*Tecnologías y redes de transmisión de datos, Enrique Herrera Pérez.*

Cada nodo tiene un receptor y un trasmisor para trasmitir los datos al siguiente equipo, sólo uno puede enviar mientras el otro está en espera, este proceso es denominado como token, de esta manera se evitan colisiones.

Ventajas

- Con esta topología de anillo se simplifica el acceso al medio.

Desventajas

- Si alguna de las estaciones no funciona, se rompe la cadena de la trasmisión.
- Para poder añadir otro host es necesario romper el anillo en un punto, causando que la red deje de funcionar.

1.3.5 TOPOLOGÍA ÁRBOL

También es llamada como topología jerárquica, la mayoría de los host están conectados a concentradores secundarios que pueden ser switches o hubs, que a la vez están conectados a concentradores primarios o un central. La topología en árbol se pude ver como un conjunto de redes en estrella conectados a un bus mediante el switch primario (Fig. 6).

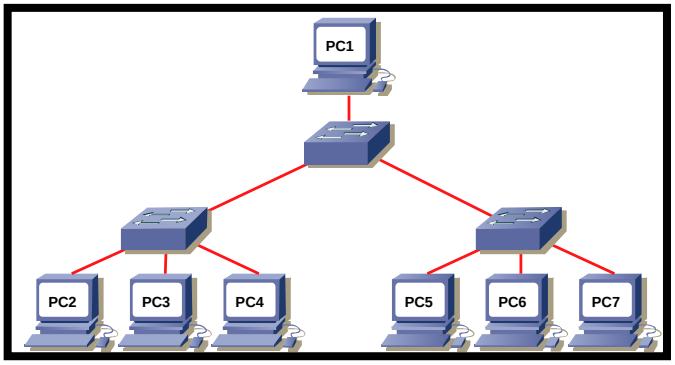

Fig. 6 “Topología Árbol” Fuente:*Tecnologías y redes de transmisión de datos, Enrique Herrera Pérez.*

Ventaja

- Facilita el crecimiento de la red.

Desventaja

- Si falla un nodo implica la interrupción de la comunicación en toda la rama del árbol que desprenden de ese nodo.

1.3.6 TOPOLOGÍA MALLA

Cada equipo se conecta a todos los demás, lo que hace posible que la información pueda viajar por distintas rutas (Fig. 7).

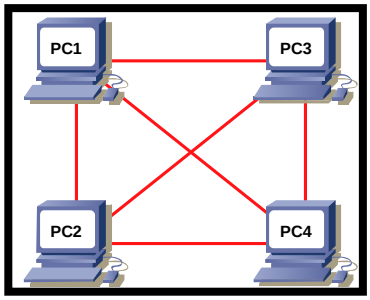

Fig. 7 "Topología Malla" Fuente:*Tecnologías y redes de transmisión de datos, Enrique Herrera Pérez.*

Ventajas

- Si algún enlace falla siempre existirán rutas alternas para entregar la información a su destino.
- Garantiza la comunicación entre los host.

Desventajas

- Es limitada la conexión de los host, de lo contrario se dispararía el número de enlaces.
- Es muy caro el cableado para interconectar todos dispositivos entre sí.

Las topologías lógicas más comunes son:

- broadcast [26]
- Transmisión de tokens[27].

[26] **Broadcast:** paquete de datos que se envía a todos los nodos de una red.
[27] **Trasmisión de token:** trama que contiene información de control. La posición de token permite que un dispositivo transmita datos en la red.

1.3.7 DISEÑO DE LA RED JERÁRQUICA

Un apropiado diseño jerárquico, es un requisito fundamental para la longevidad de una red local de datos, el administrador de red debe ser capaz de reconocer una LAN, bien diseñada seleccionando los dispositivos apropiados de acuerdo a las necesidades y recursos con los que cuenta, para así poder obtener los beneficios al adoptar un diseño de red jerárquico.

Beneficios de una red jerárquica.

- Escalabilidad.
- Redundancia.
- Seguridad.
- Administración.
- Mantenimiento.

La gran ventaja de implementar el diseño jerárquico (Fig. 8) es que la red se puede ver como divisiones, es decir, como capas independientes y cada capa cumple funciones específicas, esto hace posible que el diseño de la red se vuelva escalable y funcional.

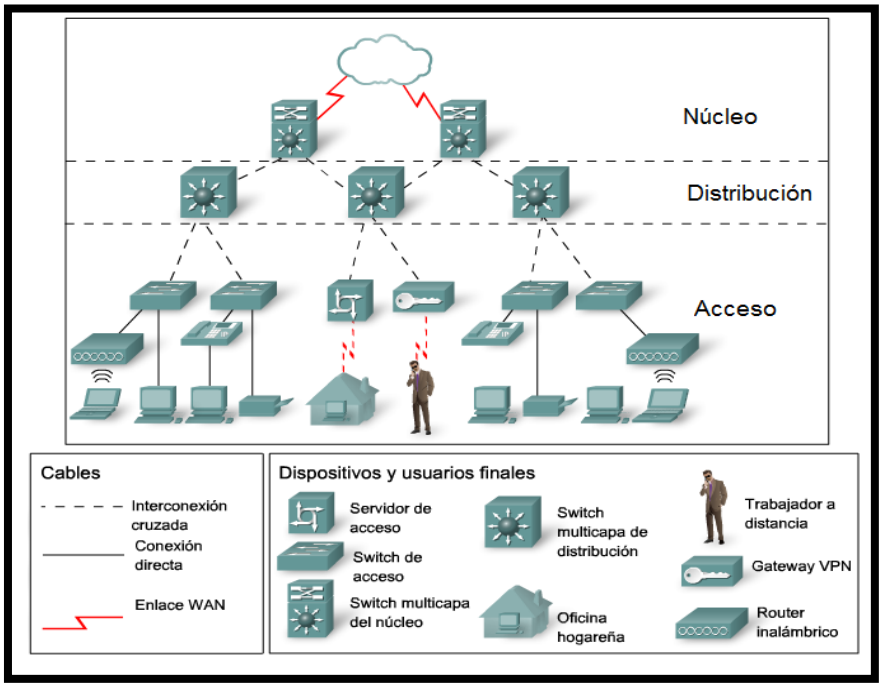

Fig. 8 "Diseño Jerárquico" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

El modelo del diseño jerárquico está compuesto por las siguientes capas:

***Capa de acceso**:* Aporta un medio de conexión de los dispositivos a la red y controla que dispositivos pueden comunicarse en la red (dispositivos finales como: PC, impresoras, teléfonos IP, access point, smartphone, etc.).

***Capa de distribución**:* Controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales definidas en la capa de acceso.

***Capa de núcleo**:* Es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante, también puede conectarse a los recursos de Internet.

1.4 CONCEPTOS FUNDAMENTALES

1.4.1 LAS CINCO OPERACIONES QUE REALIZAN LOS SWITCHES LAN ETHERNET

***Aprendizaje**:* Las tablas MAC de cada Switch debe completarse con las direcciones MAC y con sus puertos correspondientes. Cada vez que no exista la entrada, el Switch la creará en la tabla MAC utilizando la dirección MAC de origen y asociara la dirección con el puerto en que llego, en este momento está completa la tabla MAC.

***Actualización**:* Las entradas de las tablas MAC se actualizan constantemente y cuando se agrega una nueva recibe una marca horaria.

***Inundación**:* Si el Switch no sabe a qué puerto enviar una trama porque no se encuentra en la tabla MAC la dirección MAC del destino, lo enviará a todos los puertos, excepto al puerto en el que llegó.

***Reenvió selectivo**:* Es el proceso por el cual es analizado la dirección MAC de destino de una trama para que saber el puerto correspondiente de la trasmisión.

***Filtrado**:* Un Switch no reenvía una trama al mismo puerto en el que llega. Para poder dividir la red en subredes es necesario el direccionamiento jerárquico que identifica cada host de manera exclusiva, la dirección lógica de IPv4 de 32 bits es jerárquica y está constituida por dos partes, la primera identifica la red y la segunda al host, se quiere de ambas partes para completar una dirección IP, dividida en cuatro grupos de ocho bits denominados octetos.

1.4.2 SEGMENTACIÓN

Rápidamente los Switches se convirtieron en una parte esencial en las redes, permitiendo la segmentación de la LAN en distintos dominios de colisión, cada puerto del switch representa un dominio de colisión diferente y ofrece un ancho de

banda completo al nodo o a los nodos conectados al puerto. Al segmentar la red en pequeños dominios de colisión se logra más ancho de banda y se tiene mejor control porque aísla el tráfico entre segmentos (Fig. 9).

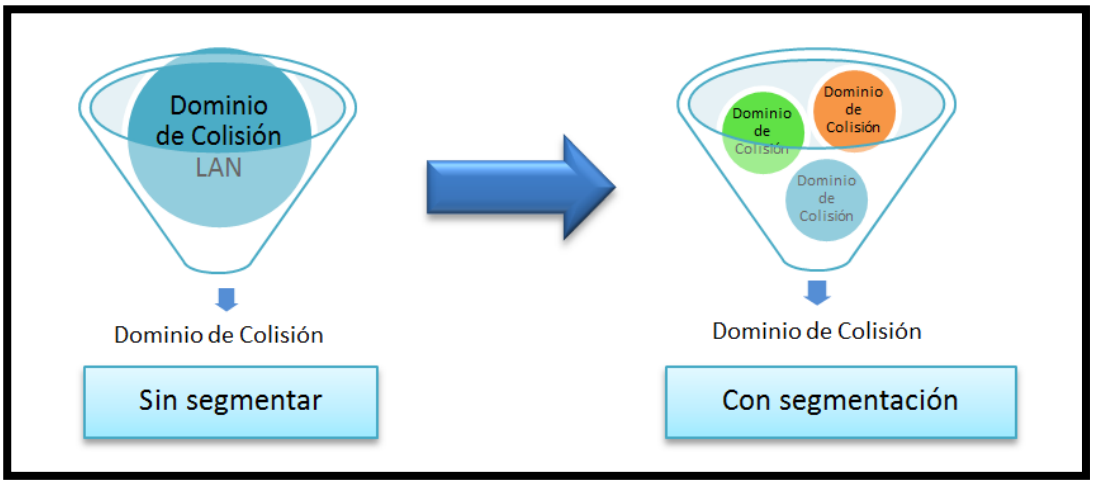

Fig. 9 “Dominios de colisión” Fuente: (creación propia, 2013).

Sin la implantación de la segmentación las grandes redes podrían embotellarse rápidamente con el tráfico y las colisiones.

1.4.3 DIRECCIÓN IP

En general las direcciones IP son utilizadas para identificar los diferentes nodos en una red. Las direcciones IP están formadas por 4 bytes (32 bits) y se pueden representar en la notación decimal, hexadecimal o binario con punto, de la forma (x.y.w.z) donde cada una las variables es un número comprendido entre 0-255, 00-FF hexadecimal o en binario desde 00000000 hasta 11111111 (Fig.10)

Direcciones IP			
32 Bit (4 Bytes)			
8 bits (1 byte)	8 bits (1 byte)	8 bits (1 byte)	8 bits (1 byte)
1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0	1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0	1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0	1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0 1 ó 0
Primer Octeto	Segundo Octeto	Tercer Octeto	Cuarto Octeto
0 – 255 decimal	0 – 255 decimal	0 – 255 decimal	0 – 255 decimal
256 de numero posibles	256 de numero posibles	256 de numero posibles	256 de numero posibles

Clase Red	N° Bits Subred / Host	Direcciones de Subred	Nº máquinas por subred que son numerables	Rango Direcciones IP
A	8/24 255.0.0.0	T) 0.0.0.0 - 127.0.0.0 R) 0.0.0.0 P) 10.0.0.0 R) 127.0.0.0	2^{24}-2=16777214	Rango válido 1.0.0.1 -127.255.255.254 Todo para uso público Internet excepto 1 Subred privada 10.0.0.1 -10.255.255.254 1 Subred reservada 127.0.0.1 -127.255.255.254
B	16/16 255.255.0.0	T) 128.0.0.0 - 191.255.0.0 P) 172.16.0.0 - 172.31.0.0 R) 169.254.0.0	2^{16}-2=65534	Rango válido 128.0.0.1 -191.255.255.254 Todo para uso público Internet excepto 16 subredes privadas 172.16.0.1 -172.31.255.254 1 subred reservada 169.254.0.1 - 169.254.255.254
C	24/8 255.255.255.0	T) 192.0.0.0 - 223.255.255.0 P) 192.168.0.0 - 192.168.255.0	2^{8}-2=254	Rango válido 192.0.0.1 - 223.255.255.254 Todo para uso público Internet excepto 255 subredes privadas 192.168.0.1 - 192.168.255.254
D y E	32/0 255.255.255.255		Multicast	

T) Total P) Privadas sólo para uso en redes privadas y no en Internet R) Reservadas para usos diversos

Fig. 10 “Direccionamiento IP” Fuente: http://88.12.10.114:8880/electron/franjagl/st/temas/IP.pdf

- Clase A: Hay 126 redes con 16,777,214 direcciones para host cada una.
- Clase B: Hay 16384 redes con 65534 direcciones para host cada una.
- Clase C: Hay 2097152 redes con 254 direcciones para host cada una.

De acuerdo al número de host que se necesiten para cada red, las direcciones de Internet se han dividido en clases A, B, C, D y E (Fig. 11). La clase D está

formada por direcciones que no identifican a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

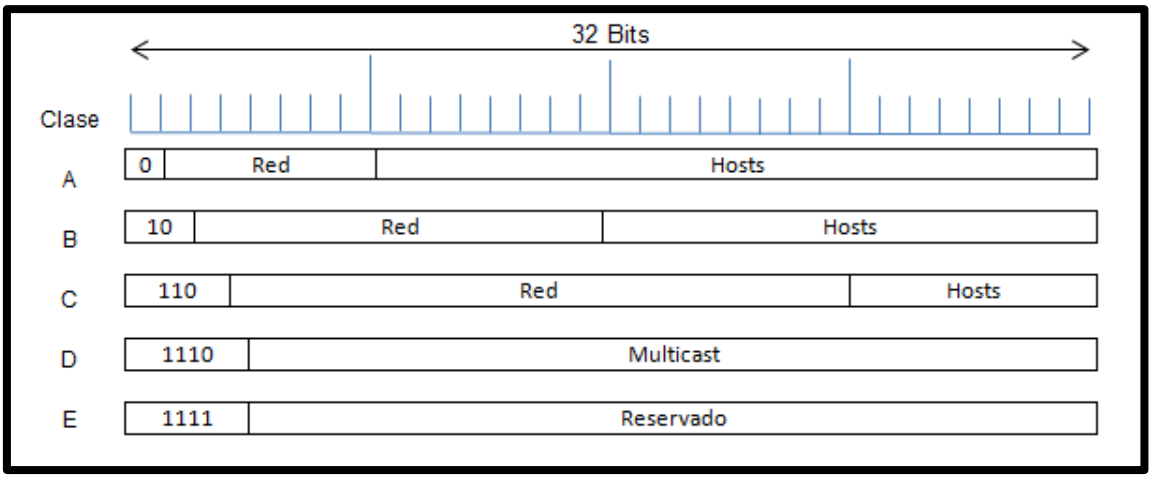

Fig. 11 “Direcciones de Internet” Fuente: http://88.12.10.114:8880/electron/franjagl/st/temas/IP.pdf

La mala asignación de direcciones IP provocó su agotamiento en su versión 4, así que se creó la IPv6 que utiliza 128 bits en lugar de 32, se representan en 8 secciones de 16 bits cada una, separadas por dos puntos y convertidas a 4 dígitos hexadecimales, por ejemplo:

A201:6dc8:8d20:79da:54fe:210a:1a2b:0acb

Actualmente está en proceso la migración de IPv4 a IPv6, muchos de los dispositivos aún no se integran por completo a esta nueva tecnología por lo tanto se sigue utilizando IPv4.

1.5 VLAN

La mayor parte del tráfico en Internet se origina y finaliza en conexiones de Ethernet. Cuando inició la fibra óptica, Ethernet adoptó esta tecnología para aprovechar el mayor ancho de banda y ofrecer un menor índice de error. Actualmente se sigue implementado Ethernet por lo siguiente:

- Simplicidad y facilidad a mantenimiento.
- Incorporar nuevas tecnologías.
- Seguridad.
- Bajo costo.
- Actualización.

Ethernet utiliza cables de UTP y fibra óptica para interconectar dispositivos, el estándar original definió el tamaño mínimo en 64 bytes y el tamaño máximo en 1518 bytes. El estándar IEEE 802.3ac publicado en 1998 amplio el tamaño permitido a 1522 bytes como máximo. Se incrementó el tamaño con la finalidad de adoptar una tecnología denominada Red de área local virtual (VLAN).

1.5.1 CARACTERÍSTICAS DE VLAN

ID de campo normal

- ID entre 1 y 1005.
- Los ID de 1002 a 1005 se reserva para token ring y FDDI los que se crean por defecto y no se pueden eliminar.
- La configuración es guardada en la memoria flash con el nombre VLAN.Dat

ID de campo extendido

- ID entre 1006 y 4094.
- Diseñado para los ISP.
- La configuración se guarda en el archivo de ejecución.

1.6 TIPOS DE VLAN

1.6.1 VLAN DE DATOS

Configurado para enviar sólo tráfico de datos propagado por los usuarios, comúnmente llamado VLAN de datos o de usuario, la separación del servicio dedicado agiliza la comunicación de datos (Fig. 12).

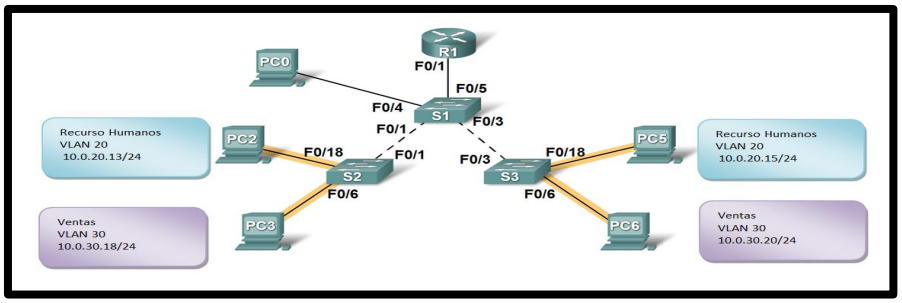

Fig. 12 “VLAN de Datos” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.2 VLAN PREDETERMINADO

Todas las interfaces hacen posible una VLAN predeterminada, la participación de todos los puertos en una VLAN predeterminada los hace parte del mismo dominio broadcast, esto hace posible que cuando un dispositivo se conecte a cualquier puerto del switch podrá comunicarse con otros dispositivos en otras interfaces del switch. Por lo general la VLAN predeterminada es la VLAN 1 (Fig. 13).

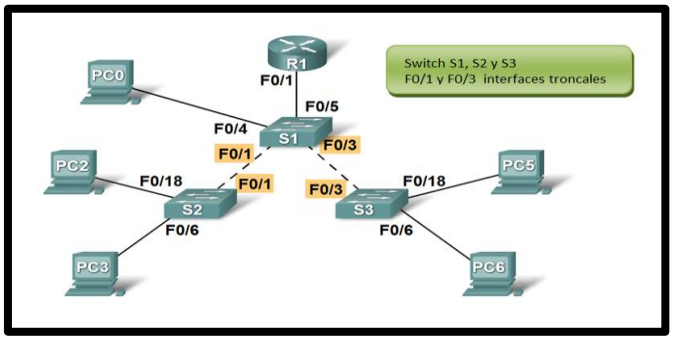

Fig. 13 “VLAN predeterminado” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.3 VLAN NATIVA

Está asignada a un puerto troncal 802.1Q. Los enlaces troncales de las VLAN admiten la transmisión de tráfico desde más de una VLAN (Fig.14).

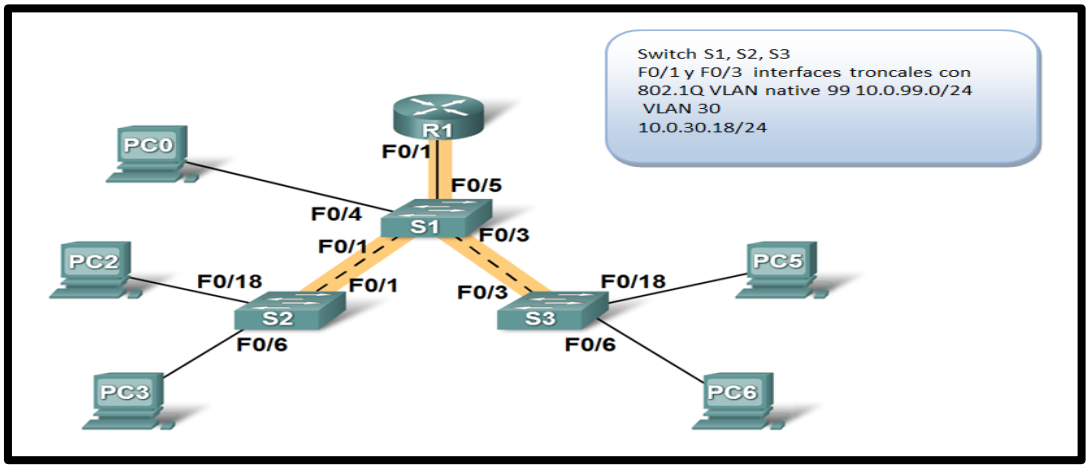

Fig. 14 "VLAN nativa" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.4 VLAN DE ADMINISTRACIÓN

Es cualquier VLAN configurable (Fig. 15) para acceder a la administración de un switch. Se asigna una IP y una máscara de subred a la VLAN de administración, además, se puede accesar mediante HTTP, SSH, telnet o SNMP.

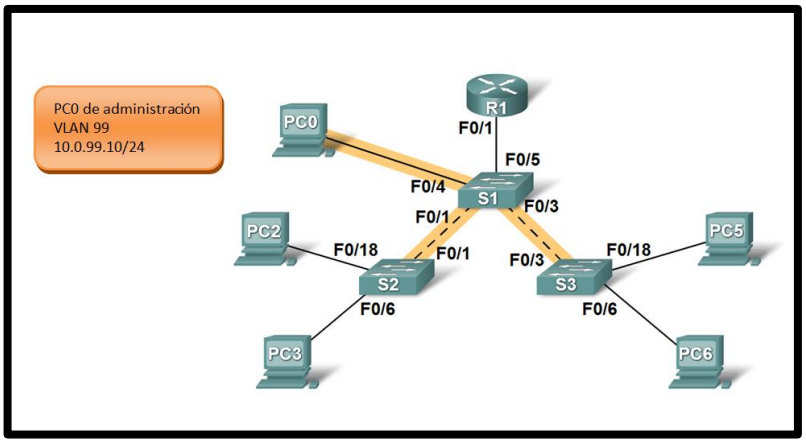

Fig. 15"VLAN de administración" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.5 VLAN DE VOZ

- Asegura la calidad de voz mediante el ancho de banda.
- Demora de menos de 150 ms a través de la red.
- Prioridad de la trasmisión sobre los demás tipos de tráfico.
- Capacidad de ser enrutador en áreas congestionadas.

Cuando se conecta el switch a un teléfono IP, el switch envía mensajes que indican al teléfono IP conectado, que envíe el tráfico de voz etiquetado con el ID de VLAN de voz.

1.6.6 RED SIN LA SEGMENTACIÓN POR VLAN

El switch cuando recibe una trama de broadcast los envía a todos los puertos, por ejemplo (Fig. 16) la PC1 envía una trama al a PC4, el tráfico que es distribuido por PC2, PC3 y S2 enseguida S1, S3, PC6, PC5 y finalmente a su destinatario PC4.

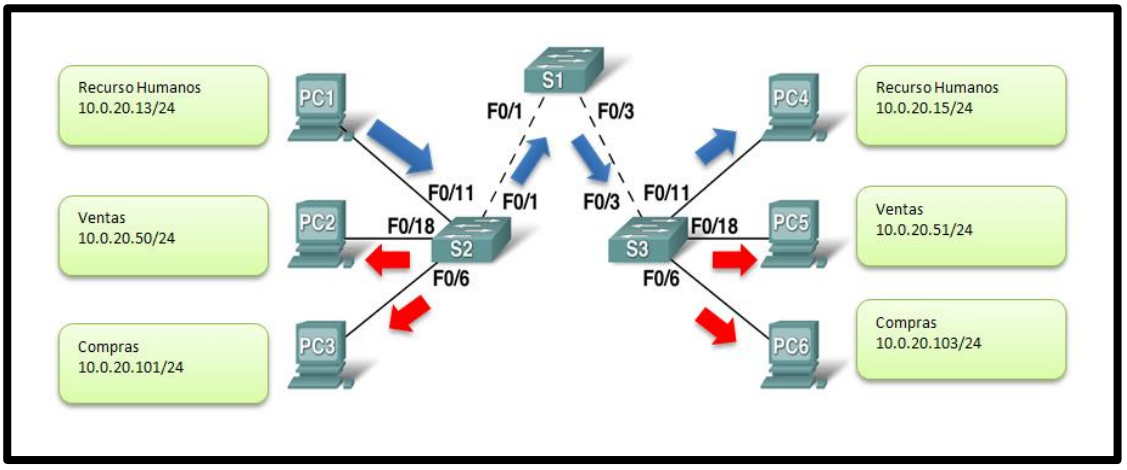

Fig. 16 “VLAN sin Segmentación” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.7 RED CON LA SEGMENTACIÓN POR VLAN

La red de la (Fig. 17) está dividida por VLAN, esto hace posible que sólo el receptor y el destinatario reciban las tramas correspondientes, evitando que los host adyacentes participen y generen tráfico innecesario en la red.

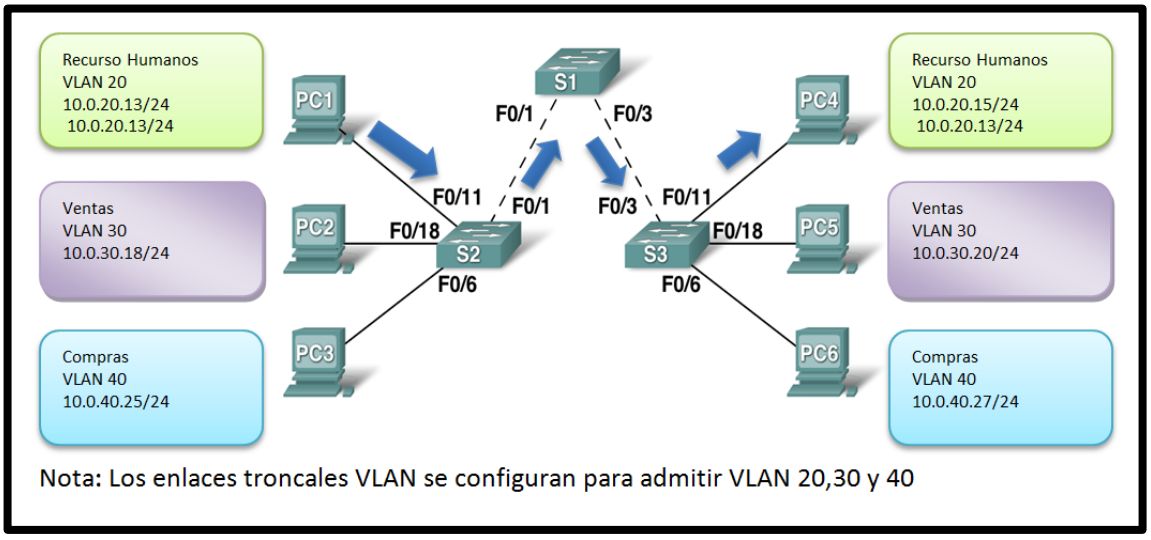

Fig. 17 "VLAN Segmentada"Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.6.8 VENTAJAS DE LA UTILIZACIÓN DE LAS VLAN

La implementación de VLAN permitirá que la red adopte y admita de manera más flexible las siguientes características:

- ***Seguridad**:* Los diferentes grupos de trabajos que tengan datos sensibles se separarán del resto de la red, para disminuir las posibilidades de que ocurran violaciones de información confidencial.
- ***Mejor rendimiento**:* La división de la red en múltiples grupos lógicos de trabajo, reduce el tráfico innecesario incrementando el rendimiento.
- ***Migración**:* El cambio de los dispositivos a la nueva arquitectura es facilitada por la división de la red en las VLAN.

- ***Administración****:* Facilita al personal de TI (Tecnologías de la información) identificar fácilmente posibles errores que pudieran existir en la red.

1.7 COMANDOS BÁSICOS PARA CREACIÓN DE VLAN

CREACIÓN DE VLAN	
Modo de configuración global.	S0#configure terminal
El ID es el numero asignado a la VLAN que se creará.	S0(config)#vlan ID
Especificar un único nombre de VLAN para identificar la misma.	S0(config-vlan)#name NombreVLAN
Se debe finalizar la sesión de configuración para que la configuración se guarde en un archivo por defaut llamado vlan.dat	S0(config-vlan)#end

CONFIGURACIÓN DE UN ENLACE TRONCAL 802.1Q Y VLAN NATIVA EN UN PUERTO DEL SWITCH	
Modo de configuración global en el switch.	S0#configure terminal
Modo de configuración de la interfaz.	S0(config)#interface interfaceID
Definir la interfaz como un enlace troncal IEEE 802.1Q.	S0(config-if)#switchport mode trunk
Configurar la VLAN 99 para que sea la VLAN nativa.	S0(config-if)#switchport trunk native vlan 99
Volver al modo privilegiado.	S0(config-if)#end

ASIGNACIÓN DE UN PUERTO DEL SWITCH	
Modo de configuración global.	S0#configure terminal
Interfaz para asignar la VLAN.	S0(config)#interface interfaceID
Definir el modo de asociación de VLAN para el puerto.	S0(config-if)#switchport mode access
Asignar el puerto a una VLAN.	S0(config-if)#switchport access vlan vlanID
Modo privilegiado.	S0(config-if)#end

Tabla 1. “Comandos básicos de los switches” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.7.1 ENLACES TRONCALES

Un enlace troncal (Fig. 18) es el enlace punto a punto que existe entre dos dispositivos de red, que transporta más de una VLAN. El protocolo IEEE 802.1Q es un modificación de Ethernet, que permite identificar a una trama proveniente de un equipo conectado a una red determinada.

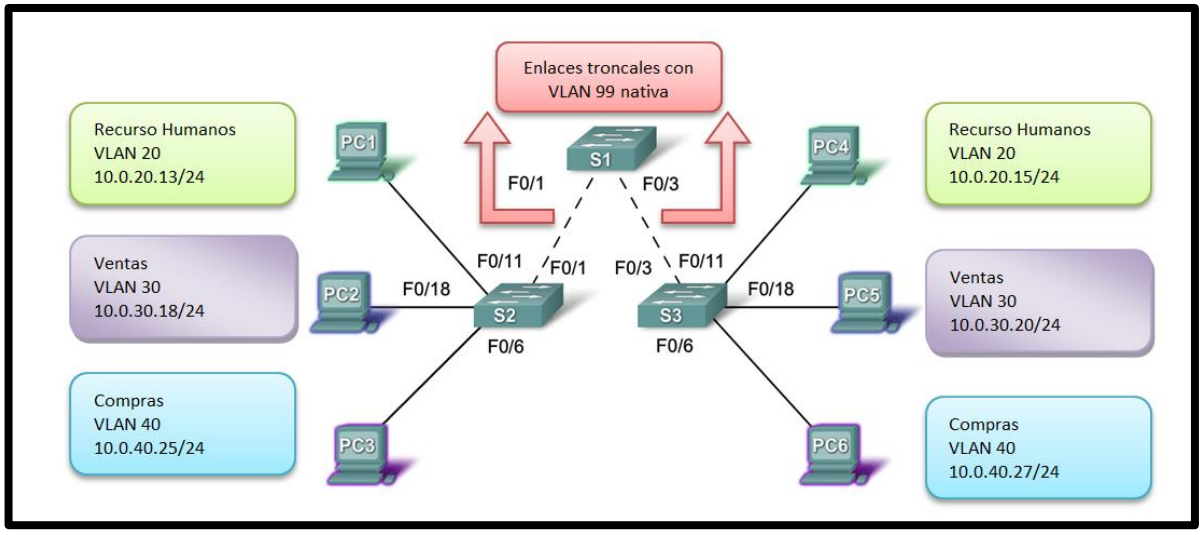

Fig. 18 "Enlaces Troncales"Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

Los enlaces troncales son los enlaces entre los switches S1 y S2 y entre S1 y S3 que deben ser configurados para admitir el tráfico de las VLAN 20, 30, 40 y 99.

1.7.2 SIN ENLACES TRONCALES DE VLAN

Se observa en el switch S1 y S2 cuatro enlaces individuales para cada segmento lo que provoca que se utilicen más puertos de los necesarios (Fig. 19).

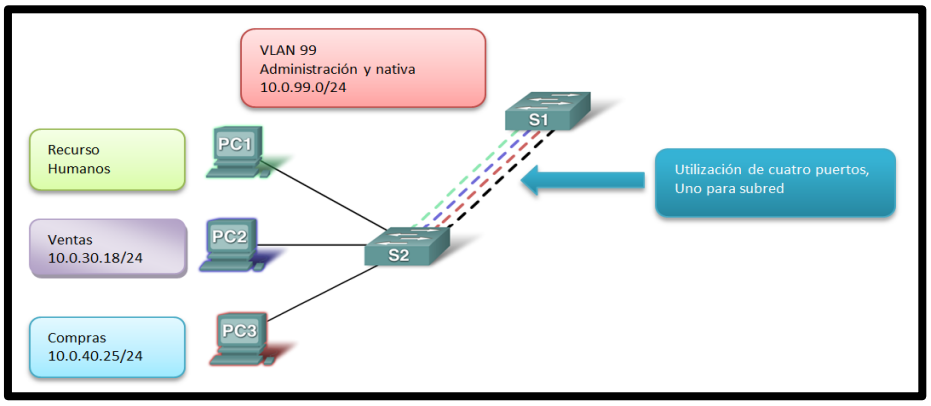

Fig. 19 "Sin Enlaces Troncales" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

1.7.3 CON ENLACES TRONCALES DE VLAN

Los switch S1 y S2 muestra un enlace troncal de la VLAN con un enlace físico único, ocupando sólo un puerto en el switch con varias VLAN (Fig. 20).

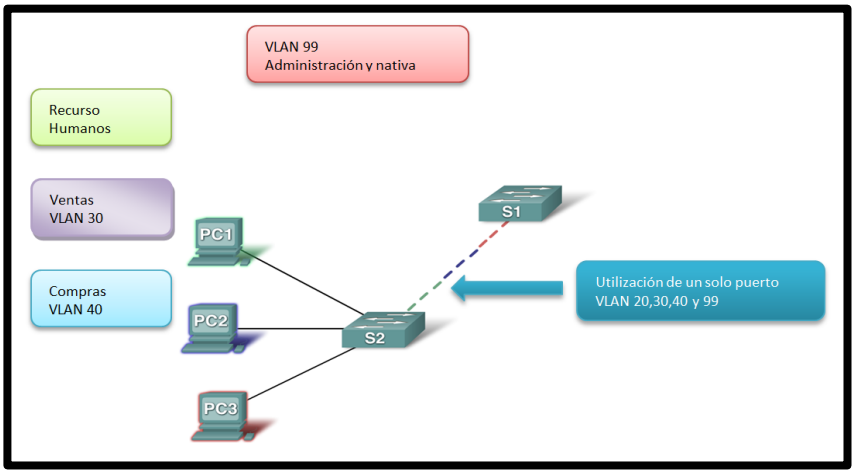

Fig. 20 "Con Enlaces Troncales" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

CAPÍTULO II
ANÁLISIS DEL PROBLEMA

CAPÍTULO II. ANÁLISIS DEL PROBLEMA

2.1 DESCRIPCIÓN DE LA RED ACTUAL

Cualquier red de datos en operación debe de contar con ciertas características esenciales para un buen funcionamiento, un aspecto primordial a considerar son las topologías que se pueden utilizar en base a las necesidades de la institución, según el rol que ésta desempeñe y de un posible crecimiento de personal.

Para el desarrollo de esta tesis, se ha contemplado implementar una nueva segmentación, utilizando la tecnología VLAN en una red con topología tipo estrella que ya se encontraba implementada, la mejora de esta red se fundamentará en la segmentación de los servicios de voz y datos, para lo cual, se describirá como se encontraba dicha red en sus inicios, que aunque no tiene implementada la segmentación por VLAN, si cuenta con ciertos parámetros que permite que dicha red funcione y opere de manera adecuada.

La red se implementará con la segmentación de VLAN para voz y datos en una red Ethernet[28], la cual, en una forma de seguridad se oculta a través de un sistema de balanceo, que se encuentra en alta disponibilidad formando un cluster, está red se encuentra implementada sobre un sistema screened o también conocido como un sistema “De-militarized”, siendo de gran utilidad para el tema de seguridad de una red.

La red del IFAI tiene una red perimétrica y su principal función es aislar el tráfico externo de la LAN interna, para prevenir una amenaza que se pudiera extender automáticamente al resto de la LAN interna. Con el objetivo de contener la amenaza e intentar aislarla en una red perimétrica, consiguiendo que él intruso que accedá a esta máquina, no consiga un acceso total a la subred protegida. Ejemplos de servicios que se pueden incluir en esta red perimétrica son elementos

[28]**Ethernet**: es un estándar de transmisión de datos para redes de área local

que deben ser visibles desde fuera de nuestra red, como páginas web y correo electrónico.

La red a implementar cuenta con una topología tipo estrella en donde un sistema de cluster activo-pasivo de corta-fuegos la segmenta, en red de usuarios, red de servidores y la DMZ. La red de área local del IFAI, tiene aplicado el principio de alta disponibilidad ya que cuenta con redundancia en la mayoría de los dispositivos de telecomunicaciones (redes), además de la disminución de únicos puntos de fallas proporcionando, al menos, una ruta más para la comunicación entre dispositivos. Esta red cuenta con un tipo de direccionamiento de red, sistemas de prevención de intrusos, traducción de direcciones y sistemas cortafuegos.

Un tema importante a considerar es el tráfico de entrada y salida hacia la nube (Internet), para ello, en la frontera con Internet se encuentran dispositivos como router y balanceadores, qué como se había mencionado se encuentran en alta disponibilidad, unas de las funciones que realizan los balanceadores son: traducción de direcciones IP hacia dentro y fuera de la red LAN, publicación de nombres de dominio de la institución, resolución de nombres de dominio(DNS[29]) de manera externa, balanceo de tráfico de entrada y salida. Estos equipos están conectados en cluster los cuales operan de modo activo-pasivo manteniendo una sincronía constante (Fig. 21).

[29]**DNS:**Domain Name System, traduce el nombre de dominio en una dirección IP para permitir al host de origen llegar el host de destino.

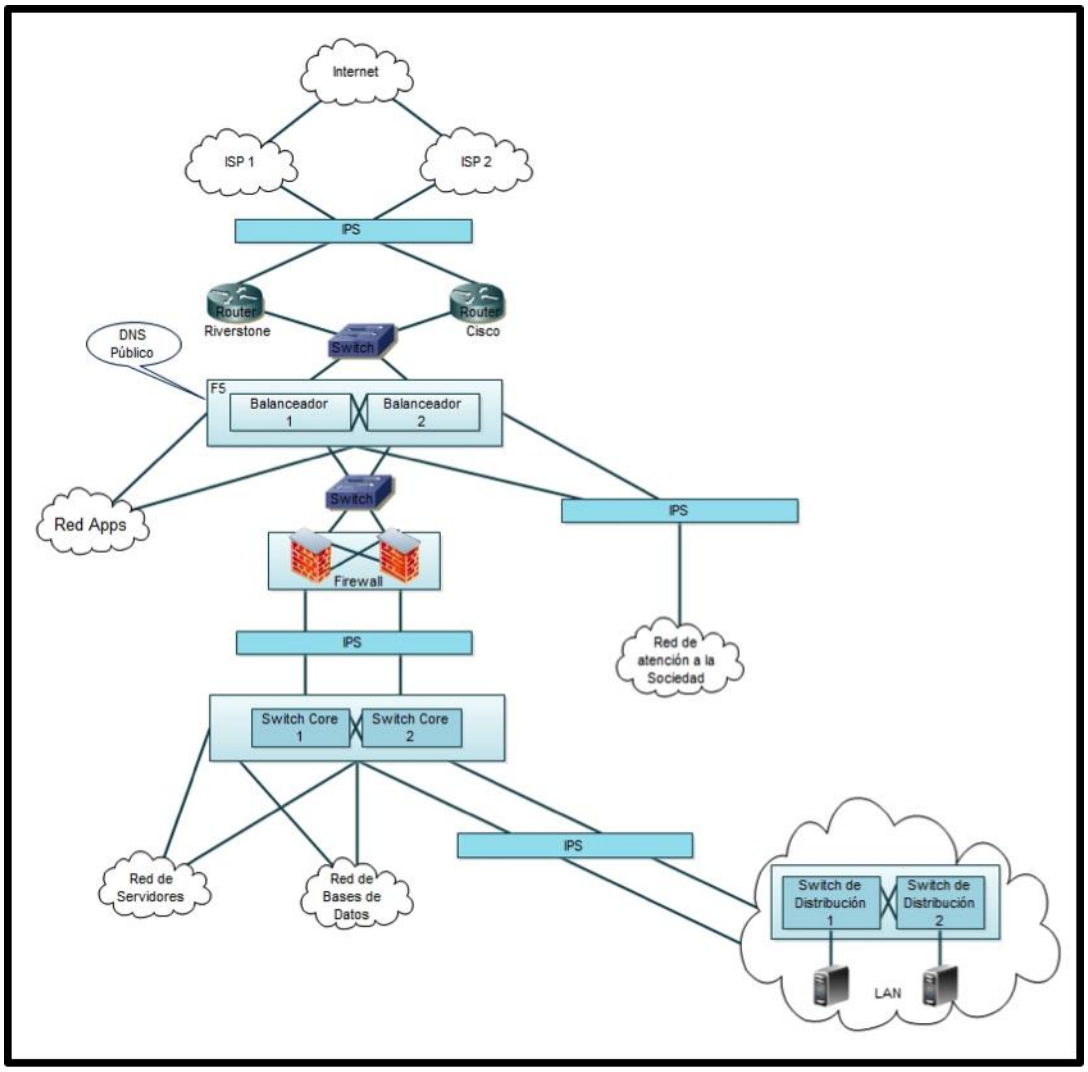

Fig. 21 “Red IFAI” Fuente: (creación propia, 2013).

También se tienen operando y conectados en cluster los sistemas cortafuegos, pero a diferencia de los balanceadores éstos, se encuentran en modo activo-activo, la diferencia entre el modo en que operan activo-activo y activo-pasivo se describe a continuación.

Cluster activo/activo: todos los nodos se encuentran dando servicio (Fig. 22).

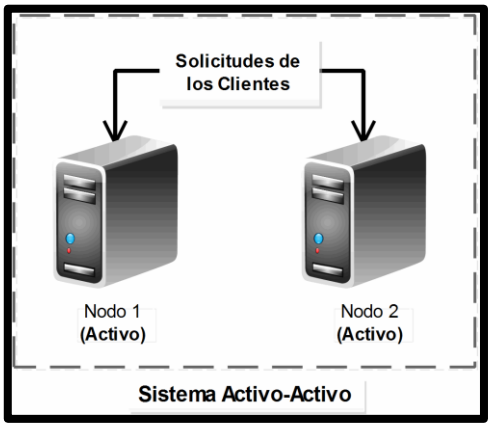

Fig. 22 “Cluster Activo - Activo” Fuente: (creación propia, 2013).

Cluster activo/pasivo: hay un solo nodo dando servicio (Fig. 23).

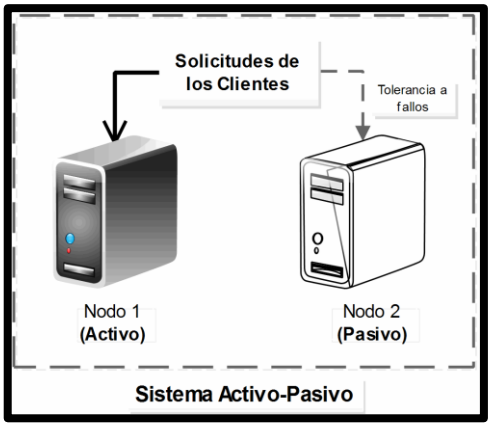

Fig. 23 “Cluster Activo - Pasivo” Fuente: (creación propia, 2013).

En la configuración modo activo-activo se debe de tener los mismos servicios en cada una de las cajas, las cuales comparten las políticas de reglas de acceso y rutas hacia los diferentes segmentos de la red, permitiendo o no los accesos de una red a otra.

Teniendo en cuenta los principios de una red jerárquica y dando la importancia que se deberá tener en la capa de núcleo, ya que es el medio de comunicación

entre los dispositivos de la capa de distribución, es indispensable que sea un medio de alta velocidad para poder reenviar grandes cantidades de datos, además de ser redundante y que se encuentre en la mayor disponibilidad, por lo tanto, se cuenta con una configuración en cluster, situada en los switches core con una configuración activo-activo en la que cada puerto está configurado como una red y VLAN independiente.

La configuración de la (Fig. 24) es idéntica en ambos equipos, ya que como se mencionó, se tiene una redundancia, por lo tanto, lo ideal es que cada servidor deberá contar con al menos dos tarjetas de red (NIC) y así estar conectado a cada uno de los switches core para asegurar, redundancia y por lo tanto, alta disponibilidad.

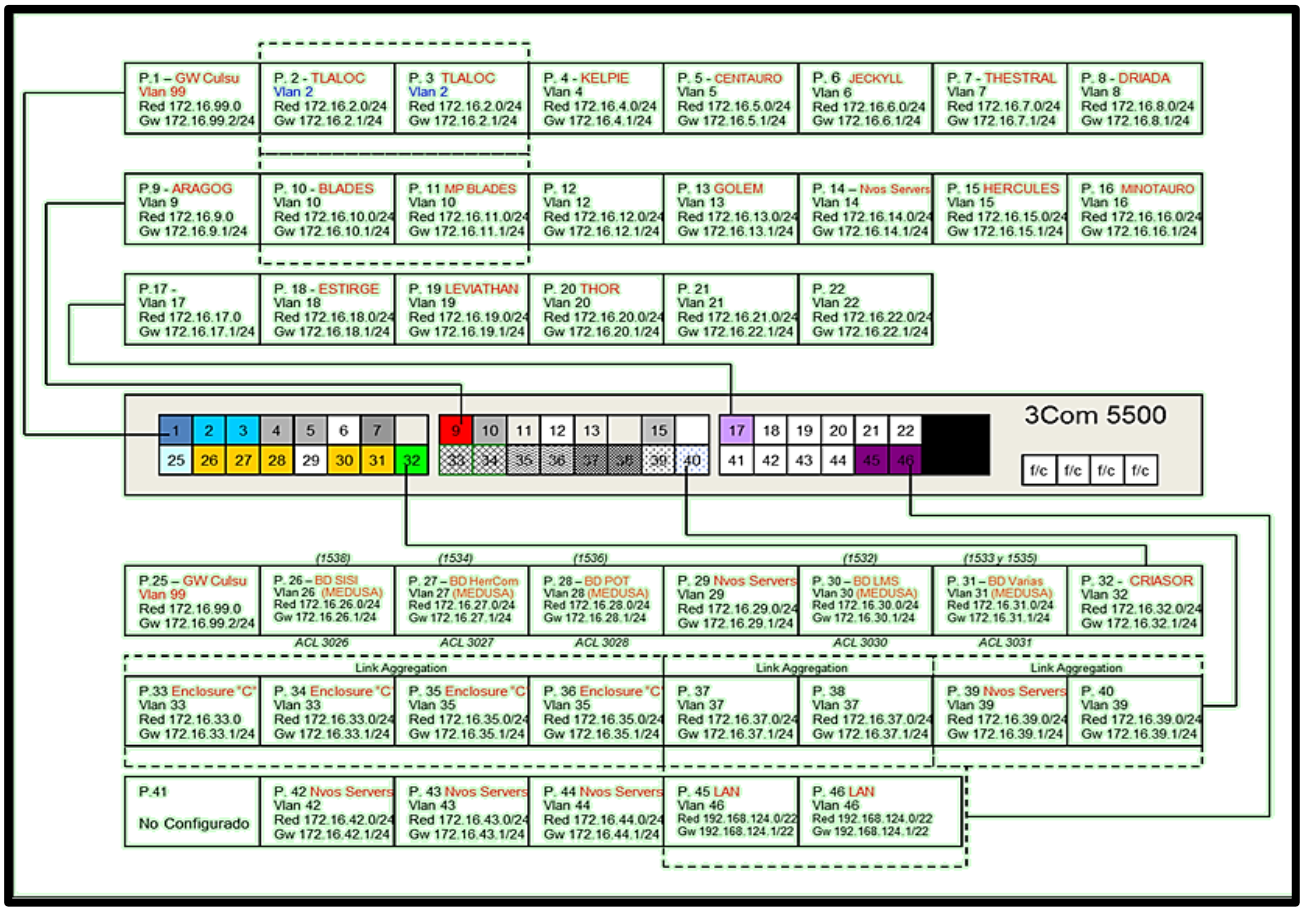

Fig. 24 “Configuración de los Switch Core” Fuente: (creación propia, 2013) .

Estos switches se definen como switches core, ya que al contar con un mayor desempeño y una mayor cantidad de puertos de alta velocidad, son responsables de mantener altas tasas de transferencia de datos en la red local del instituto. Estos switches por las características mencionadas están conectados a servidores de aplicación, equipos de respaldos y red de usuarios.

Continuando con el modelo de red jerárquica, tenemos la capa de distribución, en la cual se cuenta con un cluster de switches, los cuales transmiten los datos recibidos de los switches de la capa de acceso, antes de que se transmitan a la capa de núcleo, para su enrutamiento final ya sea dentro de la misma LAN o hacia Internet, estos switches son el backbone de la red de usuarios, ya que cuentan con puertos de fibra óptica, que se conectan a los IDF distribuidos en cada uno de los pisos del instituto.

Ya habiendo explicado las capas de distribución y núcleo de un modelo de red jerárquica, sólo resta la capa de acceso, la cual realiza la comunicación con dispositivos finales como, las PCs, impresoras, teléfonos IP y access points, los cuales se conectan un switch que por medio de fibra óptica, se comunican con la capa de distribución, con este método se asegura y mantiene el modelo de red jerárquica la cual facilita la expansión y administración de una red LAN, además de resolver posibles problemas con mayor rapidez por su separación en módulos ayudando a identificarlos.

Algunas de las características que se han fortalecido en la red del instituto, son la redundancia, alta disponibilidad y seguridad. El diseño actual, fué pensado para dar servicio a servidores de aplicación y usuarios, cuidando que al menos se tengan dos dispositivos por cada punto crítico de comunicación, por ejemplo en los sistemas de balanceo de tráfico, sistema de corta-fuegos, sistema de prevención de intrusos, switches de datos, etc.

El tema de seguridad en la red se basa en un direccionamiento de enmascaramiento no frecuente, traducción de direcciones IP para salida a Internet, un sistema de políticas de seguridad en firewall, configurado con una política restrictiva,la cual, niega todo el tráfico excepto el que esta explícitamente permitido, se cuenta con un sistema de prevención de intrusos, en el cual, se han protegido los segmentos de entrada y salida a Internet, el tráfico entre switches core y el firewall, una red exclusiva para público en general, tráfico de entrada y salida de la red de usuarios, además del acceso restringido a los equipos de telecomunicaciones.

2.2 DESCRIPCIÓN DE UNA RED PLANA

Se considera una red de topología plana, a la red compuesta únicamente por switches o hubs (actualmente ya no se utilizan los hubs debido a la baja velocidad de funcionamiento y las altas probabilidades de colisiones llegando a provocar deterioro e incluso comprometiendo la operación de la red), una de las razones por las cuales se sigue ocupando esta topología a pesar de los inconvenientes, es la facilidad y el bajo costo de implementación ya que todos los host están ubicados en la misma red; por lo tanto, la adición de un nuevo host o de otro dispositivo es relativamente fácil.

La red actual de voz y datos del Instituto se encuentra operando bajo una topología de direccionamiento IP “plana”, es decir, un direccionamiento en el que no se considera la segmentación por medio de VLAN de los diferentes servicios, como voz y datos, por lo que, todos los dispositivos de la red trabajan bajo un mismo dominio de broadcast o difusión, haciendo que la comunicación de datos sea propensa a problemas de disponibilidad y lentitud en el servicio, mientras que para la voz, es posible tener degradación de la calidad en el servicio debido a la carga de tráfico, generado por los usuarios en un solo dominio de broadcast.

El direccionamiento IP empleado para proporcionar servicio de red de datos y servicio de voz a los usuarios en el Instituto, es como el que se muestra en la (Tabla 2).

N° Piso	Rango de direccionamiento IP	Mascara de Red	N° direcciones IP para asignar	Tipo de Servicio
PB a 5	192.168.122.1 - 192.168.124.254	255.255.252.0	1022	Datos y Voz
Piso 6	192.168.6.1 - 192.168.6.254	255.255.255.0	254	Datos y Voz

Tabla 2. “Direccionamiento IP de Datos” Fuente: (creación propia, 2013).

El segmento de red 192.168.122.0/22 permite asignar hasta 1022 direcciones IP y siendo utilizadas de forma indistinta para la asignación de servicios de datos y telefonía.

El segmento de red 192.168.6.0/24 permite asignar hasta 254 direcciones IP, utilizadas de forma indistinta para la asignación de servicios de datos y telefonía exclusivamente para el piso 6, este direccionamiento fue necesario debido al aumento de personal del instituto.

Nota: El rango de direccionamiento IP 192.168.6.1 – 100 es para servicio de datos; mientras que el rango 192.168.6.101 – 200 es para servicio de telefonía en el piso 6.

2.3 VENTAJAS DE LA RED ACTUAL

Como todo el tráfico es manejado bajo una misma topología de red IP “plana”, la configuración para brindar los servicios, tanto para voz y datos es relativamente sencilla.

El equipamiento de telecomunicaciones (switches), que proporciona los servicios de acceso a la red en el Instituto, no tiene configuración avanzada, por lo que la

instalación y puesta en marcha es muy simple, debido a que operan con la configuración de fábrica.

2.4 DESVENTAJAS DE LA RED ACTUAL

A medida que la demanda de acceso a la red en el Instituto comienza a crecer, ésta se vuelve cada vez menos eficiente. Esto debido a que el tráfico de la red incrementa provocándole congestión, y por ende, el rendimiento de la red disminuye, además que al aumentar el número de dispositivos y aplicaciones, los tiempos de respuesta se degradan, provocando lentitud.

El diseño del direccionamiento IP empleado actualmente, para soportar los nuevos requerimientos de acceso a la red de datos de la Institución ya no es suficiente. Esto es porque el direccionamiento IP actual se ha agotado no permitiendo la escalabilidad de la red.

Al emplear un mismo esquema de direccionamiento IP para los servicios de datos y voz, provoca que la calidad del servicio de telefonía, sea susceptible a la congestión en la red, dando como resultado, que la calidad de la voz se degrade considerablemente.

El limitado diseño de red, incrementa la posibilidad de fallas en la red derivadas por el incremento de tráfico (congestión) y pérdida de la disponibilidad de los servicios de datos y voz. Esto trae como consecuencia, un incremento en el costo de los servicios de soporte; además, limita la implantación de nuevas soluciones y aplicaciones para la institución.

En este tipo de diseño de red, es difícil aplicar políticas de seguridad, ya que no existen segmentos en la red que permitan la aplicación de una política entre los

elementos que conforman la red. Además, todos los elementos en la red pertenecen al mismo dominio de broadcast.

Como el equipamiento de telecomunicaciones (switches) no cuenta con alguna configuración avanzada, es decir, opera con la configuración de fábrica, se pone en riesgo la disponibilidad y la integridad de los datos y la voz.

2.5 REQUERIMIENTOS

En esta etapa se requiere principalmente de la infraestructura de capa 2 y 3 del modelo OSI, para la implementación de los nuevos segmentos de red en la institución.

También es importante contar con el cableado estructurado adecuado para el correcto funcionamiento de los servicios de voz y datos en el Instituto.

La asignación del direccionamiento IP, tanto para voz y datos, se podrá realizar de forma manual o a través de servidores DHCP, este último solo se mencionará como alternativo sin llegar la implementación debido a extenso que puede abarcar el tema.

El ruteo para la comunicación entre VLAN debe ser realizado por los dispositivos de capa 3 (switches core o router).

2.6 ALCANCE

El desarrollo de esta tesis incluye los siguientes componentes de la infraestructura tecnológica del instituto (Tabla 3).

- Conectividad de dispositivos a red de datos a través de conexión UTP.
- Servicio de voz a través de terminales IP.

SERVICIO	COMPONENTES
Conexión UTP	Suministro, conexión y configuración de los equipos de telecomunicaciones. Suministro de infraestructura y accesorios necesarios para su instalación (donde sea necesaria).

SERVICIO	REQUERIMIENTOS ESPECÍFICOS
Conexión UTP	Ethernet Categoría 6 Terminador (plug) RJ-45 y Jack necesario Velocidad de transmisión 10/100/1000 BaseT PoE para los puertos que así lo requieran Soporte a voz y video

SERVICIO	COMPONENTES
Terminales de voz IP	Suministro del terminales VoiP en tres niveles de equipos: • Ejecutivo • Estándar • Operativo

SERVICIO	COMPONENTES
Equipos core	Intercambio de datos Ethernet Capa 3 Puertos RJ45 Capacidad de VLAN Capacidad de Ruteo Capacidad de ACL Llegadas de fibra óptica para conectar pisos Puertos Necesarios para interconectar pisos, servidores, dispositivos, aplicaciones y servicios. 10/100/1000 Base T.

Tabla 3. “Servicios” Fuente: (creación propia, 2013).

2.6.1 DESCRIPCIÓN DE LOS EQUIPOS Y SERVICIOS A CUBRIR

- Equipos para servicios de datos.
- Equipos para servicios de voz IP.

2.6.2 DIAGRAMA DE LA SOLUCIÓN CONSIDERANDO LOS EQUIPOS DE CONECTIVIDAD

En la (Fig. 25) se muestra el diseño de la red para la interconexión de los usuarios, para este caso en particular se tomó como base una red jerárquica, con una capa de núcleo colapsado, sin dejar de considerar un ambiente inalámbrico, el cual no se desarrollará en este tema de tesis, ya que se ha basado exclusivamente en la segmentación de los servicios. Pero se sugiere se mantenga un esquema similar en el diseño de una red.

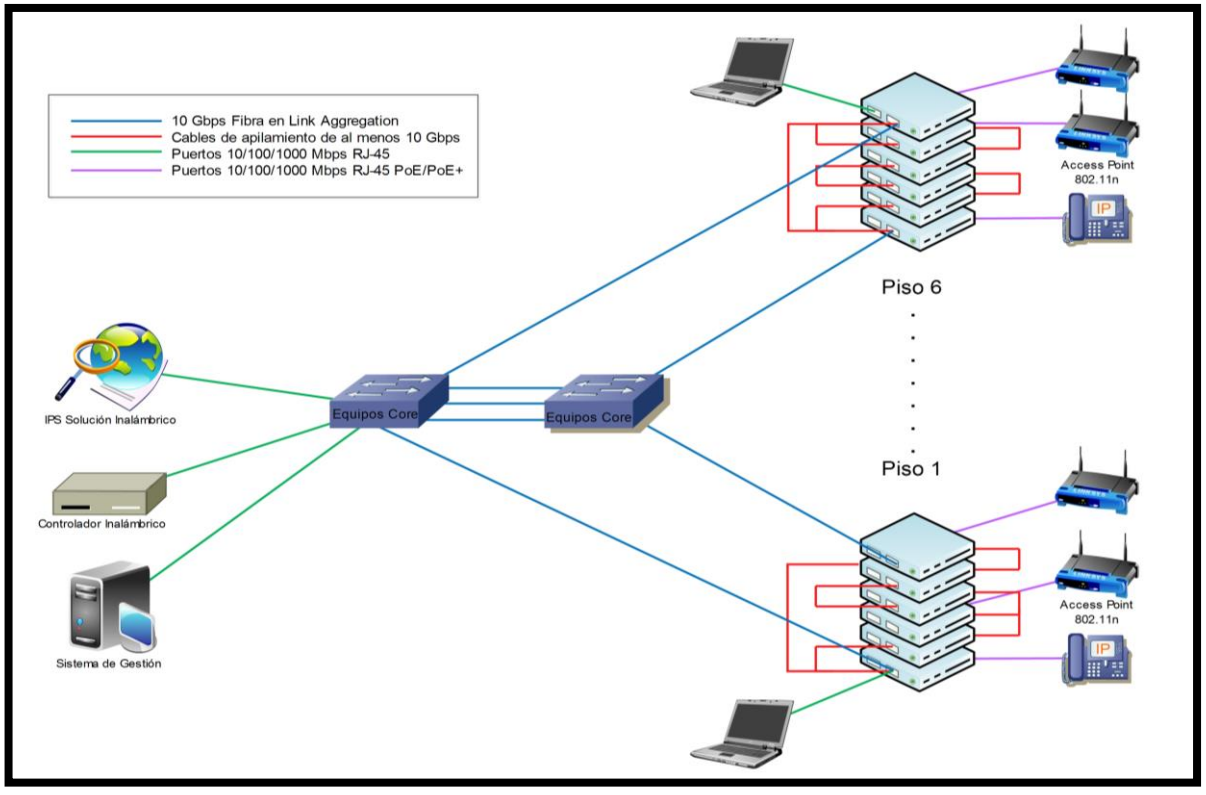

Fig. 25 “Interconexión Usuarios” Fuente: (creación propia, 2013).

2.6.3 DIAGRAMA DE LA SOLUCIÓN EN EL CENTRO DE DATOS

Se diseñó la red se ha propuesto de forma tal, que los usuarios y servidores tengan una segmentación física y lógicamente visible, con el fin de tener un mejor control en la seguridad y administración de los mismos. En ambas soluciones se utilizó la tecnología de switches apilables (Fig.26), el cual provee escalabilidad para un posible crecimiento futuro, rendimiento en el ancho de banda entre switches debido a un cable especial backplane, con lo cual reduce los posibles problemas de cuello de botella hacia la capa de distribución o núcleo, en nuestro caso núcleo colapsado (combinación de capa de distribución y núcleo en un solo dispositivo).

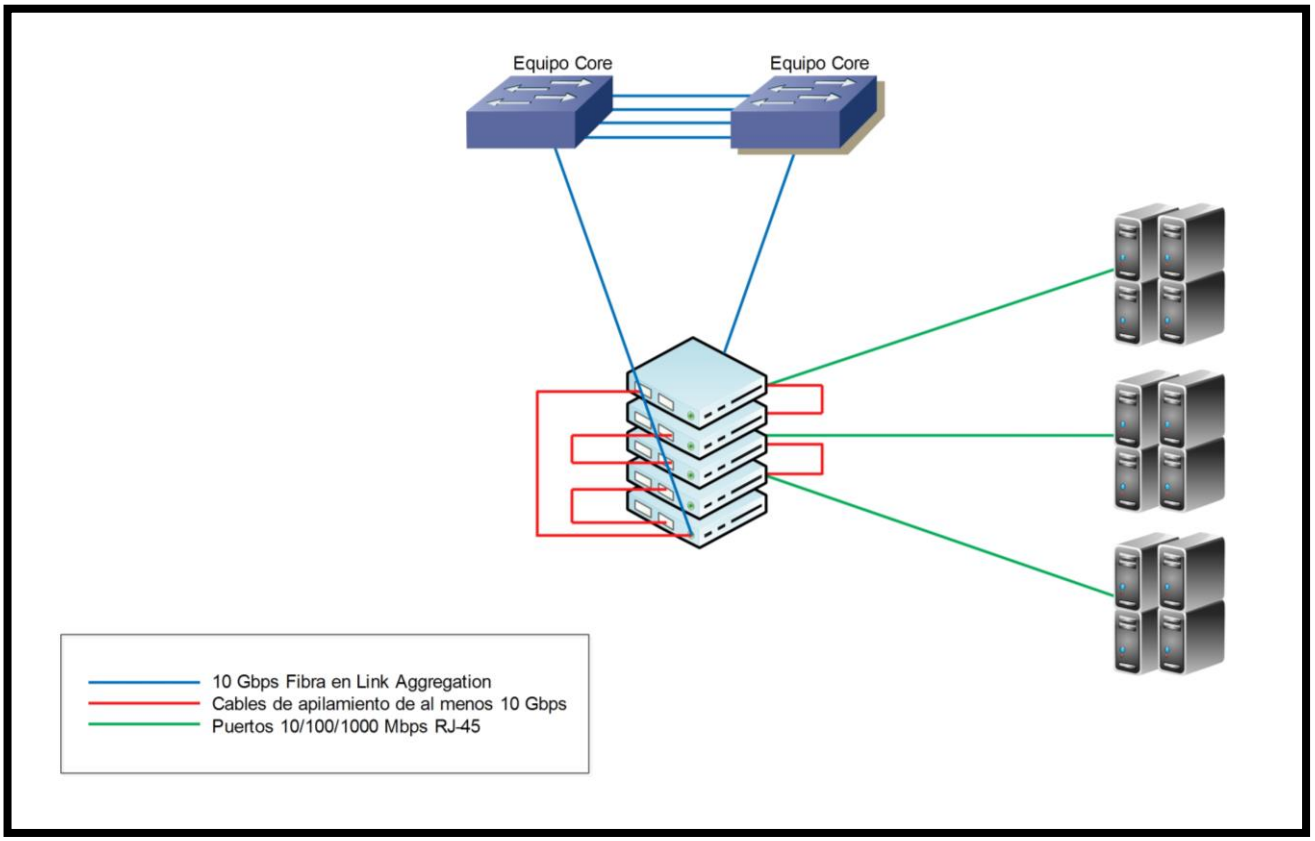

Fig. 26 “Centro de Datos” Fuente: (creación propia, 2013).

Características que debe contar el equipo switch de Acceso (Tabla 4).

SWITCH DE ACCESO
Generales • Deberá de contar con 24 puertos 10/100/1000 Base Tx autosensados con tecnología MDI/MDI-X, cuatro de estos puertos deberán soportar tecnología de 1000 Base SX. • Deberá contar con soporte mínimo de dos puertos de 10GbE y al menos dos puertos dedicados para apilamiento de 16Gbps. • Deberá contar con un desempeño mínimo de 152 Gbps y 114 Mbps. • Deberá contar con 2 puertos Stackeables de 10 GBps cada uno. **PoE** • Deberá soportar los 24 puertos con PoE Clase 3 (15.4 W). • Deberá soportar 802.3at o el estándar PoE+ soportando al menos 24 dispositivos. • Deberá contar con sensores de temperatura para su monitoreo. **Redundancia** • Deberá contar con redundancia en fuentes de poder interna con tecnología hot-swap y balanceo de carga. • Redundancia en ventiladores (opcional). **Administración** • Deberá poder configurarse por medio de un puerto de consola con interface RS-232. • Podrá configurarse por medio de una sesión de Telnet para accesar el Command Line Interface del equipo. • SSH v2. • Bitácoras del sistema. • Bitácora de Syslog. • El Software del sistema y el de los módulos de servicio deberá poder ser migrado a nuevas versiones de manera remota y local dentro de las instalaciones del cliente vía protocolo TFTP y SCP. • Autenticación local de usuarios sobre sesiones de Telnet y SSH para actividades de administración en el equipo. • El equipo deberá ser capaz de guardar una bitácora de eventos. • Capacidad de salvar y restaurar la configuración total del equipo. **Capa 2** • Deberá de soportar un mínimo de 32,000 direcciones de MAC, así mismo se requiere que se soporte un número mínimo de 254 instancias de STP. • Deberá permitir la creación de hasta 4,000 VLAN. • Deberá poder crear VLAN basadas en protocolo (802.1v), subred, puerto y dirección de MAC. • Debe aceptar configuraciones de vlan duales y soportar VLAN de voz (voice-vlan) **Capa 3** • El equipo deberá de contar con las siguientes funcionalidades de ruteo: 1. Soporte para al menos 16,000 rutas en Hardware. 2. Ruteo de subredes directamente conectadas. 3. Rutas estáticas.

4. RIP v1/v2.
5. OSPF v2.
6. Ruteo de multicast.
7. Virtual Interfaces.

Apilamiento

- Deberá ser capaz de configurarse en apilamiento de hasta 8 dispositivos con las siguientes características:
  1. La interconexión del apilamiento deberá de contar como mínimo con un desempeño de 40 Gbps.
  2. La interconexión del apilamiento deberá usar puertos dedicados para ello.

Seguridad

- Deberá contar con soporte a 802.1x con la siguientes extensiones:
  1. Autentificación de múltiples usuarios por puerto.
  2. Asignación dinámica de VLAN.
  3. Asignación dinámica de filtros en configuración de múltiples usuarios por puerto.
  4. Asignación de filtros de direcciones de MAC en configuración de múltiples usuarios por puerto.

- El equipo deberá soportar listas de acceso en capa 2, 3 y 4 por medio de:
  1. Puerto físico.
  2. Dirección MAC fuente/destino.
  3. Información de VLAN.
  4. Protocolo capa 3.
  5. Dirección IP fuente/destino.
  6. Protocolo IP capa 4.
- Las tareas de filtrado (listas de control de acceso) deberán realizarse a nivel de Hardware y no de Software para garantizar el desempeño del switch.

Compatibilidad

Para garantizar la compatibilidad de los equipos, el equipo deberá contar con el soporte a los siguientes protocolos:

- IEEE
  1. 802.1d-1998 Bridging
  2. 802.1q/p VLAN Tagging and Priority
  3. 802.1w Rapid Spanning Tree
  4. 802.3 Ethernet
  5. 802.3ad Link Aggregation (Dynamic and Static)
  6. 802.1v Protocol VLAN
  7. 802.3af Power over Ethernet

Tabla 4. “Switch de Acceso” Fuente: (creación propia, 2013).

Características que debe contar el equipo switch de distribución (Tabla 5).

SWITCH DE DISTRIBUCIÓN
General • Deberá de contar con 48 puertos 10/100/1000 Base Tx autosensados con 1 **Apilamiento** • Deberá ser capaz de configurarse en apilamiento de hasta 8 dispositivos con las siguientes características: 1. La interconexión del apilamiento deberá contar como mínimo con un desempeño de 40 Gbps. 2. La interconexión del apilamiento deberá usar puertos dedicados para ello. 3. La pila de dispositivos deberá de ser administrada con una sola dirección de IP. **Seguridad** • Deberá contar con soporte a 802.1x con la siguientes extensiones: 1. Autentificación de múltiples usuarios por puerto. 2. Asignación dinámica de VLAN. 3. Asignación dinámica de filtros en configuración de múltiples usuarios por puerto. 4. Asignación de filtros de direcciones de MAC en configuración de múltiples usuarios por puerto. • El equipo deberá soportar listas de acceso en capa 2, 3 y 4 por medio de: 1. Puerto físico. 2. Dirección MAC fuente/destino. 3. Información de VLAN. 4. Protocolo capa 3. 5. Dirección IP fuente/destino. 6. Protocolo IP capa 4. • Las tareas de filtrado (listas de control de acceso) deberán realizarse a nivel de Hardware y no de Software para garantizar el desempeño del switch. • Los equipos deberán contar con soporte de seguridad en puerto a nivel dirección de MAC (Port Security). **Compatibilidad** Para garantizar la compatibilidad de los equipos, el equipo deberá contar con el soporte a los siguientes protocolos: • IEEE 1. 802.1d-1998 Bridging 2. 802.1q/p VLAN Tagging and Priority 3. 802.1w Rapid Spanning Tree 4. 802.3 Ethernet 5. 802.3ad Link Aggregation (Dynamic and Static) 6. 802.1v Protocol VLAN **Administración del tráfico.** • Límite en el flujo de entrada basado en ACL y políticas para el tráfico Límite basado en tráfico broadcast, multicast y unknown unicast

Tabla 5. “Switch de Distribución” Fuente: (creación propia, 2013).

Características que debe contar el equipo switch core (Tabla 6).

SWITCH CORE
General • Deberá de contar con 8 slots cada uno capaz de soportar 24 puertos de 1 Gb. • Mínimo 64 puertos de 10Gbps Line Rate, Non-blocking • Deberá soportar SFP+ ópticos. • Capacidad de 1.28 Tbps en switch fabric. • Capaz de dar un desempeño de enrutamiento de 960 millones de pps. • Hasta 384 puertos de 1 GbE. • Redundancia en las fuentes de poder. **Estándares IEEE.** • 802.3-2005 CSMA/CD. • 802.3ab 1000BASE-T. • 802.3ae 10 Gigabit Ethernet. • 802.3x Control de flujo. • 802.3ad Link Aggregation. • 802.1Q Virtual Bridged LANs. • 802.1D MAC Bridges. • 802.1w RSTP. **Capa 3** • OSPF v2. • RIP v1/v2. • IPv4 Multicast. • RFC 791 IP. • RFC 792 ICMP. • RFC 793 TCP. • RFC 783 TFTP. • RFC 826 ARP. • RFC 768 UDP. • RFC 1812 Requerimientos para equipos con Ipv4. • RFC 854 TELNET. **Seguridad** • ACL capa 2 y capa 3. • Contabilidad de ACL (inbound y outbound). • Ruteo basado en políticas basado en Hardware. • SSH v2.
ÓPTICOS
Se solicitan los siguientes conectores en fibra óptica • 24 conectores 10GBASE-SR para la etapa de core. • 4 conectores 10GBASE-SR para la etapa de distribución.

Tabla 6. “Switch Core” Fuente: (creación propia, 2013).

2.6.4 EQUIPOS PARA SERVICIOS DE VOZ IP

Se ha propuesto una solución integrada, flexible y escalable, de última generación, que brinde servicios de comunicación IP de alta disponibilidad. Estos servicios deberán ser provistos de manera integral y garantizar su operación óptima y transparente.

La arquitectura para comunicaciones de voz, deberá ser híbrida de control distribuido y servicios centralizados que elimine puntos únicos de falla y refuerce la estructura operativa del instituto, eliminando situaciones derivadas de fallas de la red de transporte y facilitando la migración y redistribución de servicios en diferentes inmuebles, con afectación mínima de la disponibilidad de los servicios.

Los equipos para servicios de voz IP solicitados deberán considerar los requerimientos en la solución (Tabla 7).

Equipo	Requerimientos
Sistema Integrado de Telefonía IP	Deberá cubrir al menos las capacidades siguientes iniciales mínimas, considerando un posible crecimiento conforme se indica: • Usuarios: 700 con capacidad a crecer a más de 1300 usuarios • Troncales E1-R2 (DID): 2 (3 máx.). • Troncales Analógicas: 6 • Correo de voz: 300 Buzones de Usuario • (6) Teléfonos Categoría D. • (441) Teléfonos Categoría C. • (206) Teléfonos Categoría B. • (10) Teléfonos Categoría A El sistema de telefonía requerido debe soportar las siguientes funcionalidades: • Realizar y recibir llamadas internas/externas. • Directorio corporativo. Cada usuario podrá consultar el directorio corporativo desde su terminal IP. • No molestar. • Reconocimiento de llamadas entrantes o ANI (Caller ID). • Llamada en espera.. • Se deberán soportar al menos ocho conferencias telefónicas simultáneas.. • Remarcado Automático (redial) al último número (mínimo cinco últimos números). • Rellamada (call back) Automática a extensión libre/ocupada. • Transferencia de llamadas. • Retención de llamadas.

TERMINALES DE VOZ IP
Se deberán considerar 4 categorías de teléfonos IP para usuarios. • Categoría “A”: Modelo Ejecutivo Alto. • Categoría “B”: Modelo Ejecutivo Medio. • Categoría “C”: Modelo Estándar. • Categoría “D”: Modelo Operativo.

Perfil	Características
1. Móvil ejecutivo	Servicio de datos y voz para un usuario ejecutivo el cual puede conectar dos dispositivos móviles de datos requiriendo servicio inalámbrico para ellos y un puerto UTP de datos. Requerirán terminal ejecutiva de voz IP Tipo A con puerto dual, soporte PoE.
2. Móvil estándar	Servicio de datos y voz para un usuario móvil que cuenta con equipo de cómputo móvil y por sus funciones requiere servicio de red inalámbrica y puerto UTP (PoE) de datos. Para voz IP se les asignará terminal con puerto dual Tipo B, soporte PoE.
3. Escritorio estándar	Usuario con requerimiento de servicios de datos UTP para computadora de escritorio y terminal de IP de voz Tipo C, con puerto dual, soporte PoE.
4. Sólo datos	Dispositivos que por su funcionamiento requiere conexión de datos para funcionar y proveer un servicio como son: impresoras, digitalizadores, multifuncionales, dispositivos de acceso, etc.
5. Sólo Voz	Servicio de voz donde se requiere terminal IP de voz Tipo D y un puerto Ethernet soporte PoE.

Tabla 7. “Servicios de voz IP” Fuente: (creación propia, 2013).

CAPÍTULO III
DISEÑO DE LA RED

CAPÍTULO III. DISEÑO DE LA RED

Es importante para lograr satisfacer las necesidades de cualquier empresa, instituto o comercio con un ambiente de red de área local, se adquiera un modelo de diseño jerárquico, el cual aumenta notablemente las probabilidades de que dicha red sea exitosa. Al comparar con otros diseños de redes existentes, una red jerárquica se administra y expande con mayor facilidad además, que está, permite resolver con mayor rapidez posibles problemas que pudieran surgir dentro del instituto.

Un diseño de rede jerárquica implica la división de la red en capas independientes o modulares. Cada capa cumple con funciones específicas que definen su rol dentro de la red de área local. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. Por ello en el diseño de esta red, se tendrá especial atención en tres capas fundamentales del modelo OSI: capa1 o capa física, capas 2 o capa de enlace de datos y capa 3 o capa de red, ya que en estas capas se concentra el diseño de una red LAN.

3.1 DESARROLLO DE UNA RED SEGMENTADA

Para el diseño de la nueva red segmentada por VLAN, se tomó como base la arquitectura de la red anterior que tenía como mayor fortaleza la redundancia y la alta disponibilidad, sin olvidar las necesidades del instituto, teniendo especial atención en el aumento de personal, aumento de aplicaciones y cambio de equipos de comunicaciones obsoletos y sin soporte para la nueva implementaciónde los servicios de voz y datos. Por ello se separaron de manera lógica los servicios, tanto como base de datos, aplicativos y usuarios, considerando en distintos segmentos cada uno de estos servicios, obteniendo una mejor administración y una rápida detección de posibles problemas sin comprometer toda la red, como es el caso en una red plana, la distribución de los servicios se muestra en la (Fig. 27).

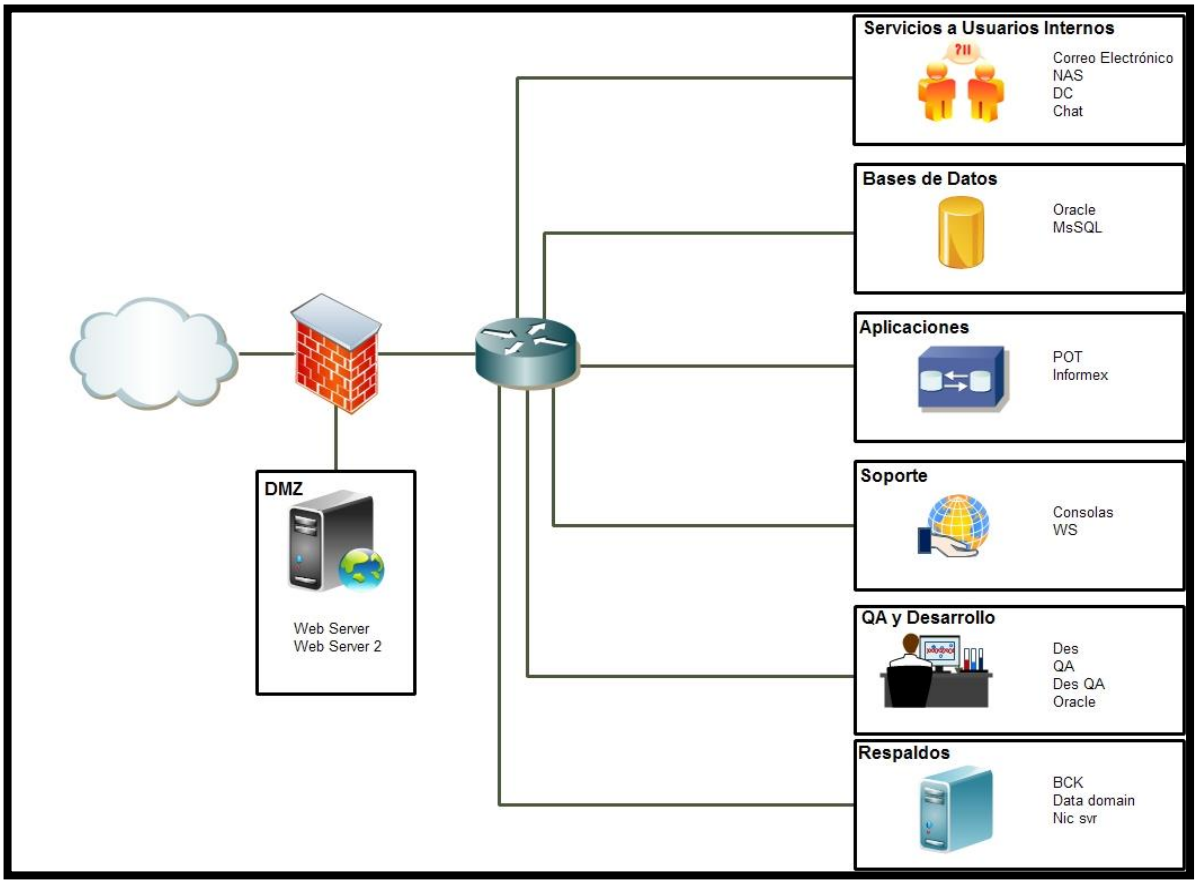

Fig. 27 “Arquitectura de la red” Fuente: (creación propia, 2014).

La propuesta contempla principalmente la segmentación de los servicios de voz y datos, para lo cual, se contemplaron nuevos segmentos de red a los existentes como se muestra en la (Tabla 8).

N° Piso	Rango de direccionamiento IP	Mascara de Red	Tipo de Servicio
PB	172.19.0.1 - 172.19.7.254	255.255.248.0	Datos
Piso 1	172.19.8.1 - 172.19.15.254	255.255.248.0	Datos
Piso 2	172.19.16.1 - 172.19.23.254	255.255.248.0	Datos
Piso 3	172.19.24.1 - 172.19.31.254	255.255.248.0	Datos
Piso 4	172.19.32.1 - 172.19.39.254	255.255.248.0	Datos
Piso 5	172.19.40.1 - 172.19.47.254	255.255.248.0	Datos
Piso 6	172.19.48.1 - 172.19.55.254	255.255.248.0	Datos
Prueba	172.19.144.1 - 172.19.151.254	255.255.248.0	Datos
VoIP	172.18.0.1 - 172.18.7.254	255.255.248.0	Voz

Fig. Tabla 8. “Segmentación IP voz y datos” Fuente: (creación propia, 2014).

Para la asignación de este direccionamiento se basó en el direccionamiento de tipo clase B establecido por la ICANN quien regula y permite asignar desde 128.0.0.0 hasta 191.255.0.0, se debe tener en cuenta que pueden existir segmento iguales asignados en otra compañías, Institutos, Universidades, etc. Por ello es importante contar con la traducción de direcciones de red (NAT) y así evitar conflictos con otras redes, a continuación en el siguiente (Tabla 9) se muestra las clases de direccionamiento IP.

Clase Red	Rango	Nº de Redes	Nº de Host por Red	Mascara de Red	Broadcast ID
A	0.0.0.0 – 127.255.255.255	128	16777214	255.0.0.0	X.255.255.255
B	128.0.0.0 – 191.255.255.255	16384	65534	255.255.0.0	X.X.255.255
C	192.0.0.0 – 223.255.255.255	2097152	254	255.255.255.0	X.X.X.255
D	224.0.0.0 – 239.255.255.255	Histórico			
E	240.0.0.0 - 255.255.255.255	Histórico			

Tabla 9. “Direccionamiento IP” Fuente: (creación propia, 2014).

Teniendo en cuenta la asignación de segmentos para los servicios de voz y datos, se consideró la cantidad de host que se asignara a cada VLAN, por ello, para el actual crecimiento del instituto, se contemplo tanto el aumento de personal como de dispositivos y utilizando una máscara de red de 255.255.248.0 (21 bits), con la cual se podrán asignar hasta 2046 direcciones IP y 32 subredes por piso, destinadas para usuarios, dispositivos de red, dispositivos de almacenamiento, servidores, etc.

Siendo los actuales requerimientos del instituto, el aumento del personal, la actualización de dispositivos obsoletos y la segmentación de los servicios de voz y datos, la asignación de la una máscara de red de 21 bits, es suficiente para la operación actual y futura que está red podría tener, el edificio cuenta con 6 pisos y un centro de datos, donde se alojan servidores y equipos de comunicaciones ubicado en la planta baja y por cuestiones de administración se considerará como un piso más, asignándole un segmento de red. Para el desarrollo e implementación del tema se tomaron varios puntos importantes como son; el diseño de capa 1, capa 2 y capa 3, que darán como resultado los procesos de instalación, configuración y pruebas.

3.2 DISEÑO DE CAPA 1

Para llegar a esta etapa inicial de diseño de una red, se deben de seguir algunos pasos que se mencionarán brevemente y aunque no es un tema que se desarrollará en esta tesis es importante resaltar. El primer punto a cumplir es la recopilación de requerimientos y expectativas de los usuarios, es decir, se debe tomar en cuenta la historia del proyecto a realizar, tanto su estado actual y su proyección a futuro. A la vez que se deberá tener un perfil de las personas que utilizarán la red.

También se deberá determinar los recursos que se tendrán disponibles, si existen operaciones críticas, los tipos de protocolos que se permitirán, los permisos que los usuarios tendrán dentro y fuera de la red local. Estos aspectos son de suma importancia ya que las operaciones críticas son claves para todo negocio y el acceso a ellas es primordial.

Una vez que se haya obtenido esta primer fase, se tendrá que realizar el análisis de requerimientos, no obstante estos no son constantes y tienden a cambiar, por ello se busca que la red sea capaz de brindar información pronta y confiable a sus usuarios, logrando el objetivo de la disponibilidad en base a los requerimientos analizados, ya que poco es de utilidad una red que da preferencia a recursos de video y audio cuando sus operaciones criticas radican en la disponibilidad y confiabilidad de páginas web, por ello es necesario priorizar y restringir los servicios, para proveer la mejor disponibilidad con el menor costo.

Otro aspecto de suma importancia es la elección del diseño de topologías. La topología física hace referencia a la manera o la configuración de computadoras, servidores cables y periféricos, mientras que la topología lógica es la manera o la forma en que una red transmite tramas[30] de un nodo a otro utilizando los medios

[30] **Trama**: unidad de envío de datos, haciendo referencia a la capa 2 del modelo OSI

físicos, para el desarrollo de la tesis, se tomará como base la topología estrella extendida ya que ésta es la utilizada por el instituto y un cambio de topología además del costo implicaría afectación a la operación del Instituto.

Para el diseño de la capa física, capa 1 en el modelo OSI, que es responsable de la transmisión de los datos entre un nodo origen y un destino, una de las decisiones en el diseño de una red es el medio y la topología a utilizar, ya que de esto depende la cantidad de información y la velocidad por el cual se transmitirá en el medio; si se eligé un medio de alto costo, en una red pequeña en la cual los requerimientos son mínimos, aunque el rendimiento de la red sea óptimo se desaprovecharían los recursos y no se cumpliría la primicia de diseñar una red a la mejor disponibilidad y con el menor costo, de igual manera si se considera adquirir un medio de bajo costo, sin considerar los requerimientos, los costos a un futuro serían más elevados que una buena adquisición desde un inicio.

El medio que se eligió en el diseño de esta red, es el cable UTP[31] categoría 6 para las conexiones entre los dispositivos, debido a su velocidad de transmisión de hasta 1 Gbps[32], su retro-compatibilidad con los estándares 5/5e y a las características que presenta para evitar la diafonía[33] y ruido. Para el caso de las conexiones, entre los equipos de la capa de acceso a los equipos de la capa de distribución, o en este caso núcleo colapsado se contempló el utilizar fibra óptica multimodo, para asegurar la disponibilidad en tiempo y forma de la información, en esta parte de la red llamada “backbone” es indispensable contar con una gran capacidad y alta velocidad del medio, para la transmisión de información entre aplicativos y usuarios locales.

[31] **UTP:** Unshielded twisted pair(en español "par trenzado no blindado") es un tipo de cable de par trenzado que no se encuentra blindado y que se utiliza principalmente para comunicaciones

[32] **Gbps:** Gigabit por segundo**,** velocidad de transmisión de información

[33] **Diafonía:** se dice que entre dos circuitos existe **diafonía**, cuando parte de las señales presentes en uno de ellos, aparece en el otro

3.2.1 CABLEADO

El cableado dentro del diseño de capa 1, es uno de los componentes más críticos para la operación de la red, por ello, es importante que sea regulado por estándares internacionales como EIA/TIA 568[34]-A que especifica, que cada dispositivo conectado a una red deberá, estar conectado con tendidos de cableado horizontal a un IDF[35] y a su vez el IDF deberá estar conectado al MDF[36] mediante cableado vertical. Las conexiones entre dispositivos finales, IDF y MDF, están reguladas por las características del medio a utilizar, como se muestra en la (Fig.28).

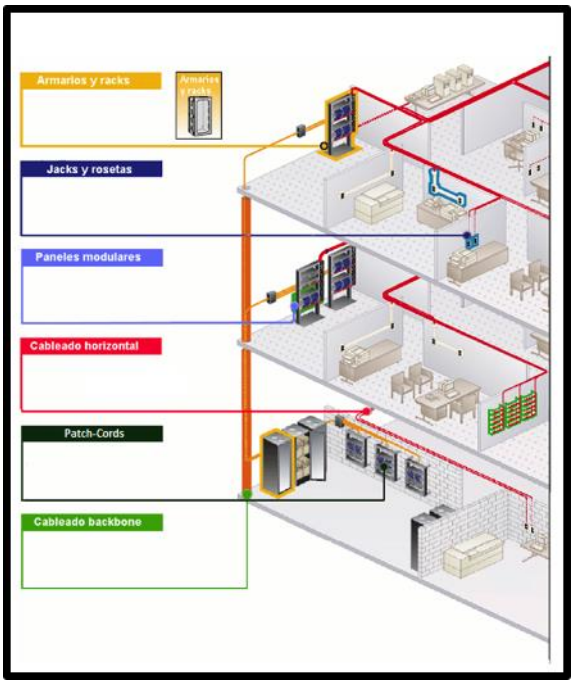

Fig. 28 “Cableado” Fuente: http://www.mainbit.com.mx/cableado.pdf

[34]**EIA/TIA:** Es un estándar que intenta definir las normas que permitan el diseño e implementación de sistemas de cableado estructurado, estas normas definen los tipos de cables, distancias, conectores y arquitecturas de sistemas cables.
[35]**IDF:**(Intermediate Distribution Frame)centro de distribución intermedia
[36]**MDF:** (Main Distribution Frame) centro de distribución principal

Medios de transmisión cable coaxial, par trenzado y fibra óptica (Tabla 10).

	Par Trenzado	Coaxial	Fibra Óptica
Ancho de Banda	Medio	Alto	Muy alto
Hasta 1 Mhz **Hasta 10 Mhz** **Hasta 20 Mhz** **Hasta 100 Mhz**	Sí Sí Sí Sí	Sí Sí Sí Sí	Sí Sí Sí Sí
Canal Full Dúplex	Sí	Sí	Sí
Distancias Medias	100 m 65 Mhz	500	2 km Multimodo 100 km Monomodo
Inmunidad Electromagnética	Limitada	Media	Alta
Seguridad	Baja	Media	Alta
Costo	Bajo	Medio	Alto
Tasa de Transferencia	Hasta 4 Mbps (4 millones de bits por segundo)	Hasta 500 Mbps (5000 millones de bits por segundo)	Hasta 2000 Mbps (2000 millones de bits por segundo; o bien 2 "giga"bps: 2 Gbps)
Estándar	T568A T568B	-IEEE 802.3 -La especificación 802.3 original utiliza un cable coaxial de 50 ohm.	Estándar Ethernet 10BASE-F 1000BASE-X Ethernet De 1 Gbit/s sobre fibra óptica.

Tabla 10. “Medios de Trasmisión”
Fuente:http://www.uv.es/~hertz/hertz/Docencia/teoria/codificacion.pdf

El diámetro de la fibra suele ser de 125µm, el diámetro del núcleo de 50/62.5µm en la fibra multimodo y 9 µm en la fibra monomodo. Se muestran las distancias máximas de un enlace para distintos tipos de fibra óptica a distintas longitudes de onda en la (Fig. 29).

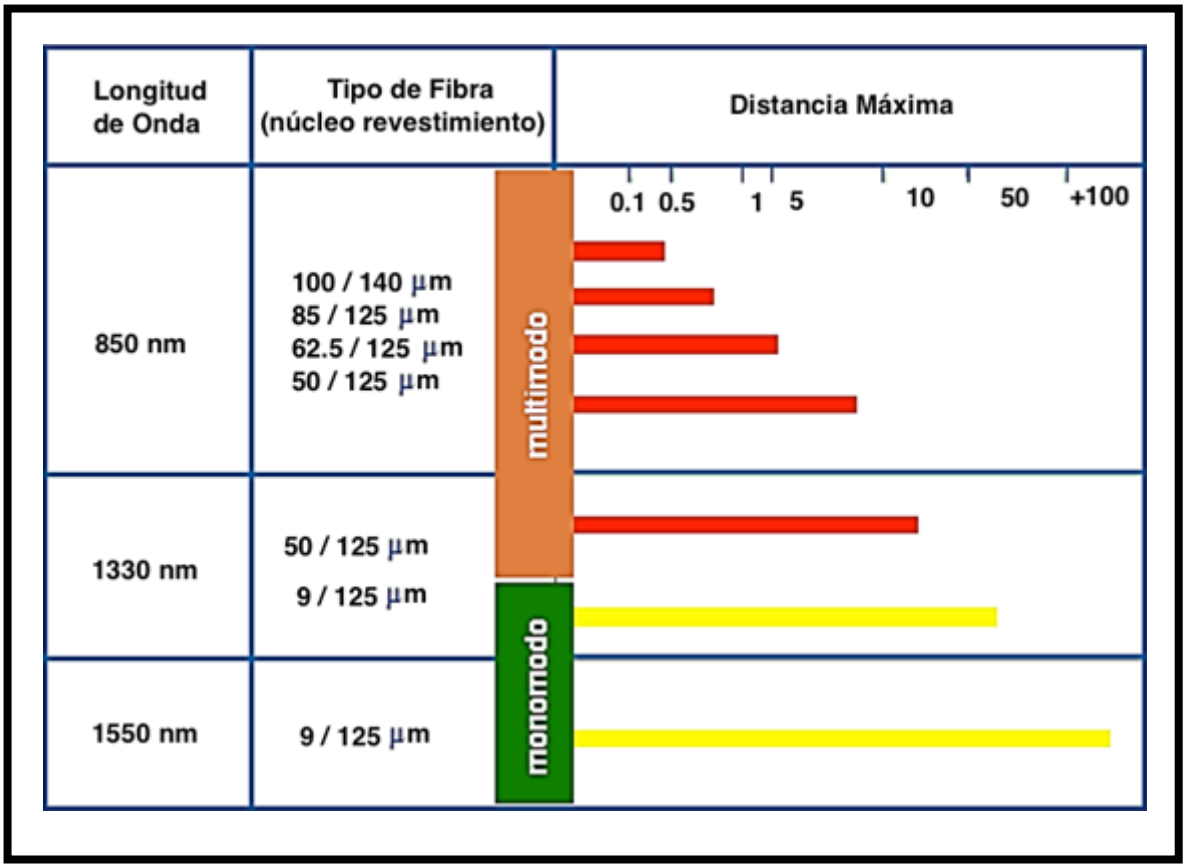

Fig. 29 “Longitud de Onda Fibra Óptica” Fuente: http://nemesis.tel.uva.es/images/tCO/contenidos/tema2/tema2_1_1.htm

3.2.2 TOPOLOGÍA ESTRELLA EXTENDIDA

En el diseño de está red, se mantuvo la topología actual que es de tipo estrella, donde un nodo es el principal y del cual dependen los demás dispositivos, para el caso de la red del instituto, el nodo principal es el firewall, en el cual todas las conexiones son procesadas. La topología tipo estrella extendida se diferencia de

la topología estrella, que uno de los nodos conectados puede ser el nodo principal de los demás equipos, esta topología generalmente se utiliza cuando los nodos de una red rebasan la limitante de 100 metros del cable UTP mostrada en la (Fig.30) “Medios de Trasmisión”, y es común que se tenga más de un IDF, dichos IDF deben de estar conectados a un MDF, mediante cableado vertical según lo establecido en el estándar EIA/TIA 568-A. Este diseño de red se mantuvo en el instituto, teniendo un IDF por piso conectandose mediante cableado vertical y debido a la limitante existente de cable UTP de 100 metros, se optó por utilizar fibra óptica que tiene un rango de hasta 2 kilómetros suficientes para la conexión vertical al MDF, estas conexiones deben ser documentadas, especificando el tipo de medio que se utiliza, la localización de cada IDF y MDF.

Diagrama de norma EIA/TIA 568-A “Estrella extendida” (Fig. 30).

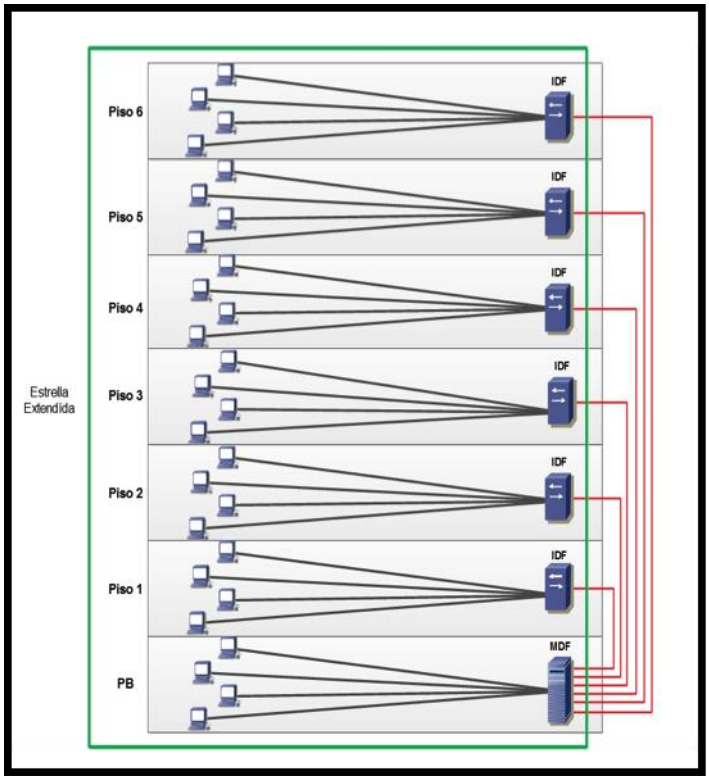

Fig. 30 “Topología Estrella Extendida” Fuente: (creación propia, 2014).

La distribución del cableado en el edificio se conservo ya que se cuenta, en cada piso con su centro de distribución intermedia (IDF) que se conecta por medio de fibra óptica al (MDF) como se muestra en la (Fig. 31).

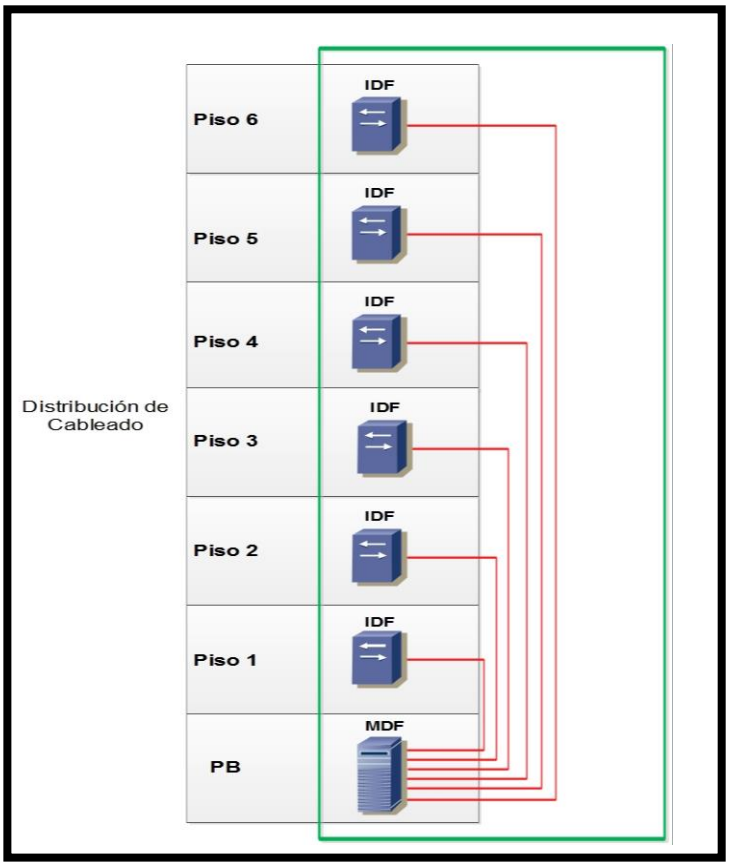

Fig. 31 “Distribución de Cableado” Fuente: (creación propia, 2014).

3.3 DISEÑO DE CAPA 2

El principal objetivo del diseño de capa 2 en una red, es el de proporcionar un control de flujo de información, detección de errores y corrección de estos, sin olvidarse de la máxima reducción de la congestión en la red, mediante filtrado de paquetes, para ello los principales dispositivos de capa 2 son los puentes y los switches, responsables de determinar el tamaño de los dominios de colisión y difusión.

3.3.1 DOMINIOS DE COLISIÓN Y BROADCAST

Un factor que se debe tener cuidado al implementar una red Ethernet[37], debido a que afectan al rendimiento, son las colisiones y los dominios de difusión. Los dominios de colisión y difusión de la red a implementar se muestran en la (Fig. 32).

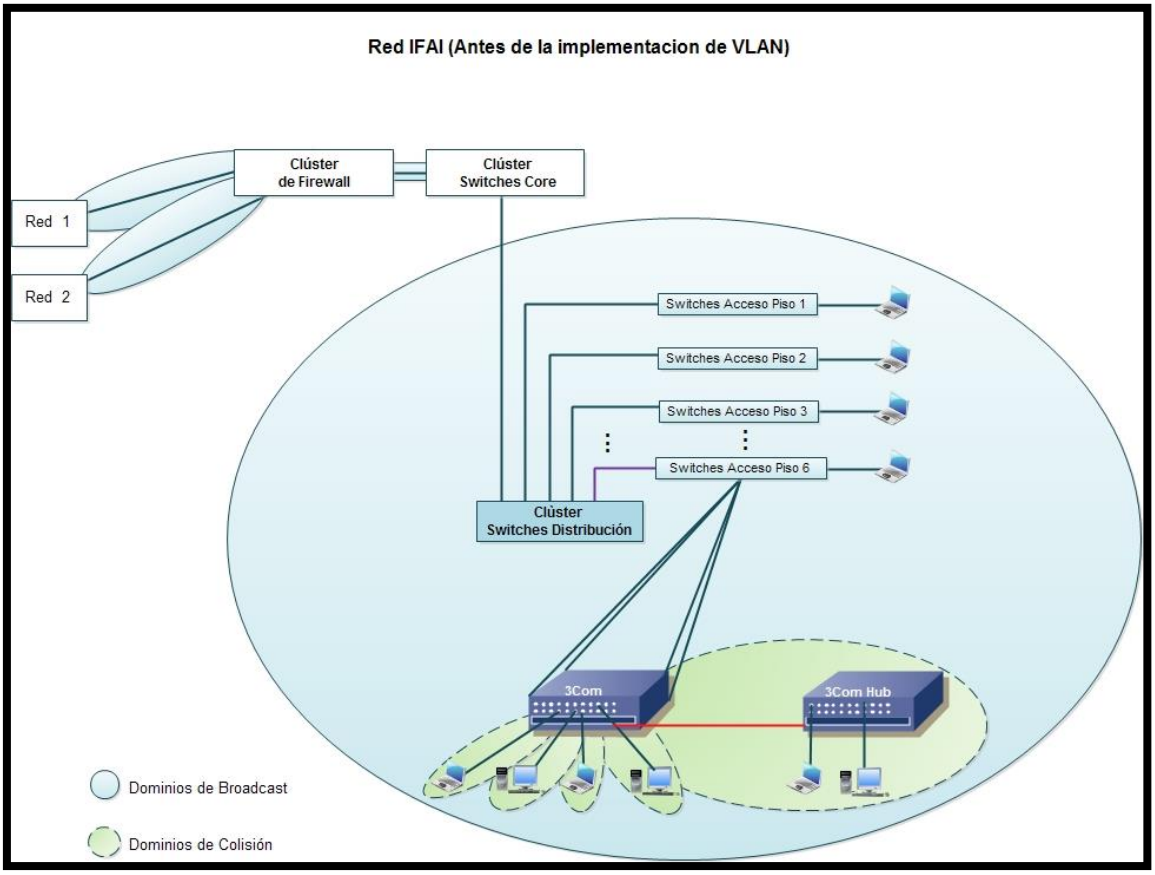

Fig. 32 “Dominios de colisión y broadcast ” Fuente: (creación propia, 2014).

Es importante identificar los dominios de colisión, para el diseño de la red ya que estos degradan el rendimiento de la misma. Los dispositivos que generan estas colisiones y además no son capaces de realizar un filtrado del tráfico de red; son los dispositivos de capa 1 como los hubs, por ello en el desarrollo de esta red se consideró, utilizar switches con lo cual se micro-segmenta la red ayudando a

[37]**Ethernet**: es un estándar de transmisión de datos para redes de área local

determinar el tamaño de los dominios de colisión y broadcast o difusión (Fig. 33) y (Fig. 34) respectivamente.

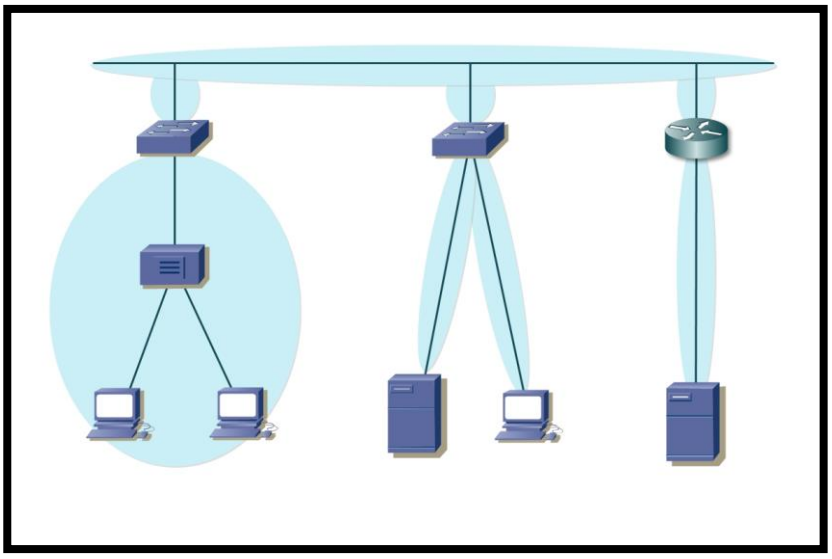

Fig. 33 “Dominios de Colisión” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*”

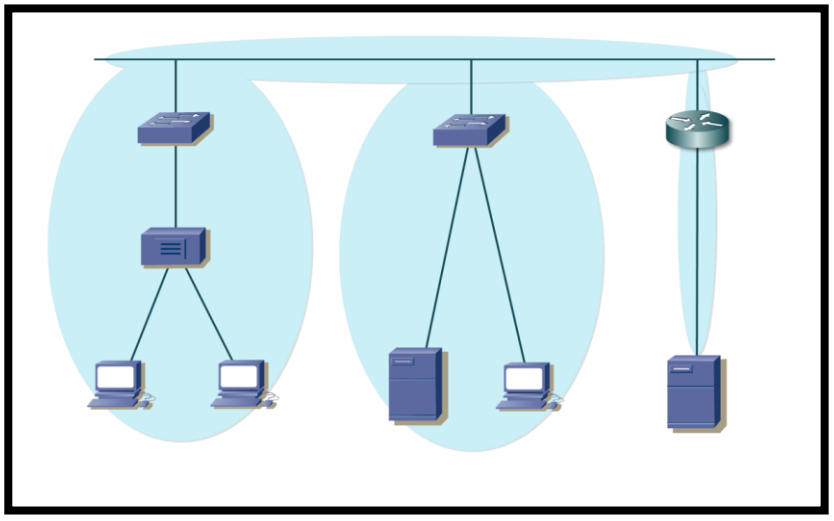

Fig. 34 “Dominios de Broadcast” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.”*

Además al utilizar switches dentro de una red LAN local, se ofrece un ancho de banda completo al nodo o a los equipos conectados.

Considerando lo antes mencionado, se han elegido dos tipos de switches, en base a los tipos de servicios que brinda el instituto como; páginas web, correo electrónico, dhcp, dns, etc. y el otro tipo de switches elegido destinado, para los usuarios, teléfonos IP y dispositivos finales. Para la conexión de los usuarios, se eligieron switches de 24 puertos con la característica PoE, esto para otorgar servicios tanto de datos como de voz en un solo cable.

Para otorgar los servicios alojados en los servidores, se consideró switches de mayor densidad de puertos sin la funcionalidad de PoE, es importante que los switches fueran asimétricos, capaces de manejar velocidades de 10 hasta 1000 Mbps, para asegurar el funcionamiento de dispositivos cuyas tarjetas de red operen a velocidades menores a 100 Mbps (Fig. 35).

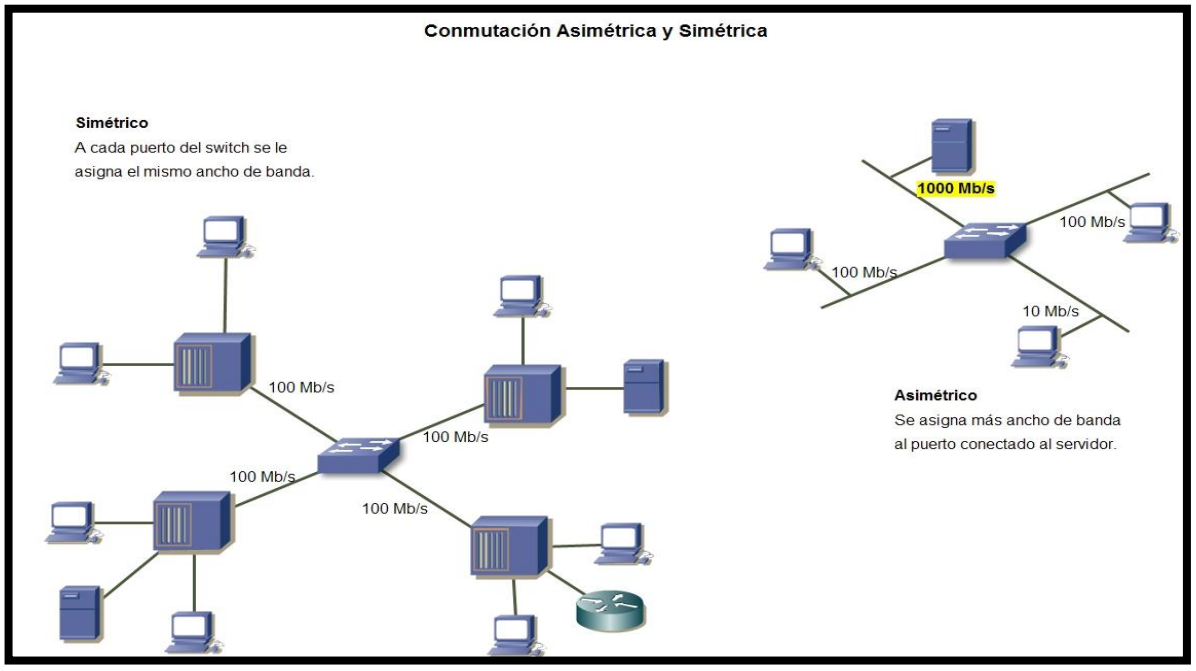

Fig. 35 “Conmutación Asimétrico” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*”

Otra característica importante en la elección de los switches, es un módulo que permita la conexión de fibra óptica requerida para el cableado vertical. Ya que de esto depende la velocidad y la capacidad de transmisión de datos y dado que en cada IDF, se tendrá configurado un stack para los switches de la capa de acceso, los módulos de fibra óptica permitirán la conexión al cableado vertical, con velocidades de hasta 10Gps asegurando un mejor ancho de banda[38] para la transferencia de datos en la red local.

En el desarrollo del proyecto se consideró el panorama ideal, donde a cada usuario le corresponde un nodo en el switch, asegurando el ancho de banda que soporte la tarjeta de red (NIC) del dispositivo, ya sea 10, 100 o hasta 1000 Mbps para cada usuario conectado al switch, se evitará dispositivos de capa 1 como hubs que además de congestionar la red, generan dominios de colisión y tiene la limitante de funcionar a la velocidad del dispositivo más lento conectado al dispositivo.

3.3.2 INCREMENTO DE LA RED

Otro aspecto que se debe tener en cuenta, es el incremento de la red, por ello, se recomienda el hecho de que la red crecerá un 100%, se deberá dimensionar al doble y no solo en las máquinas conectadas sino en toda la infraestructura como; dispositivos de seguridad, switches de capa de núcleo, switches de capa de distribución, enlaces de Internet, espacio a utilizar para la instalación de nuevos rack, etc. Pero si al momento no es posible contar con esos requerimientos, al menos, tener en cuenta equipos que soporten añadir módulos, para cambios de acuerdo a las necesidades que se presentarán en el instituto.

[38] **Ancho de Banda**: tasa de transferencia de datos - la cantidad de datos que se puedan llevar de un punto a otro en un período dado (generalmente un segundo).

3.4 DISEÑO DE CAPA 3

La principal característica en el desarrollo de esta capa, es la creación y comunicación de segmentos basados en direccionamiento IP y la segmentación de la red de área local (LAN) de manera lógica, uno de los principales dispositivos que realizan estas funciones son; los router y los switches de capa 3.

Dado que el proyecto a desarrollar solo se enfocará a un ambiente local y debido al diseño de núcleo colapsado que se utilizó en el instituto, se consideró ocupar switches de capa 3 para las tareas de ruteo y creación de ACL para la seguridad de la red LAN.

3.4.1 IMPLEMENTACIÓN DE EQUIPOS CAPA 3

Los equipos de capa 3, son los responsables de elegir el mejor camino disponible para la entrega del paquete con base al direccionamiento IP, para darle salida por el puerto que tenga el segmento indicado en el paquete, que ya previamente el dispositivo de capa 3 revisó y analizó.

Para esté caso en particular, el equipo que tendrá la mayor carga de tráfico es el switch de capa 3, teniendo funciones en el modelo de redes jerárquico de la capa de núcleo; responsable de la interconectividad tanto local como externa, también realizará las funciones de la capa de distribución, que controla el tráfico mediante VLAN permitiendo segmentarlo en subredes diferentes, este equipo de capa 3 realizará una función primordial que será la creación de reglas ACL, políticas las cuales restringirán el accesos a servicios como; bases de datos, aplicaciones, correo electrónico, etc.

El switch de capa 3 tendrá en una configuración altamente disponible y redundante, por ello, se consideró tener dos equipos de las mismas características tanto físicas como de configuración, para así evitar una interrupción en la

operación del instituto, al quedar uno de ellos fuera de operación. Estos dispositivos de capa 3 tendrán conexión con el cableado vertical de cada uno de los pisos (backbone) y se encontrarán en el MDF debido que es el punto donde se concentrará el tráfico.

Diagrama de conexión física de los equipos de capas de núcleo, distribución y acceso (Fig. 36).

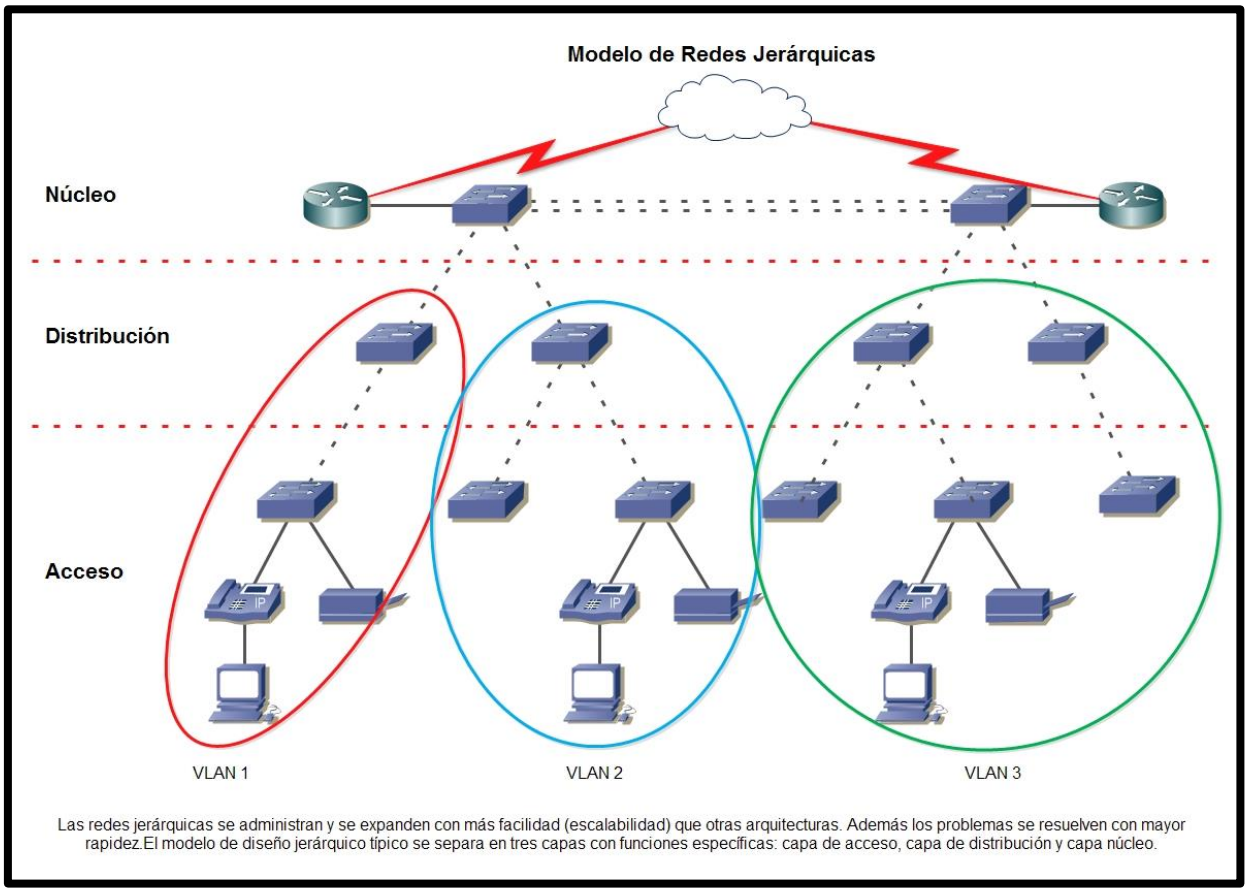

Fig. 36 "Modelo Jerárquico" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*"

3.4.2 IMPLEMENTACIÓN DE VLAN

Un factor que se debe considerar y que se debe tener especial énfasis, ya que es el tema en el cual radica el proyecto es en la creación de VLAN, tecnología que permite crear dominios de difusión más pequeños reduciendo considerablemente afectaciones en la red local, una característica que hace viable y atractiva la implementación de VLAN es la mejora en el aspecto de seguridad en la red local, permitiendo crear grupos de VLAN según su función, por ejemplo como se muestra en la siguiente (Fig. 37) donde se puede diferenciar las áreas de trabajo en una misma red local.

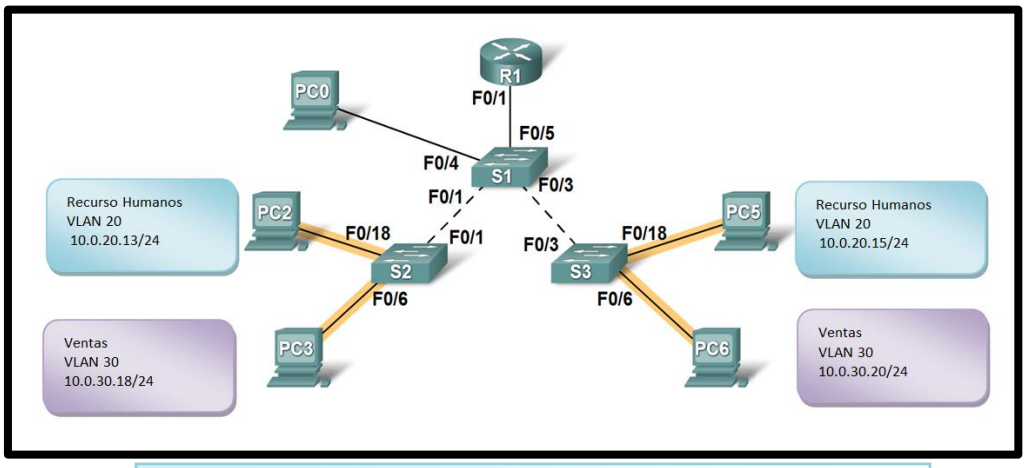

Fig. 37 "VLAN" Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN*

Para nuestro proyecto, la implementación de VLAN se desarrolló en 7 pisos, un segmento dedicado al MDF y el servicio de voz, la asignación sería de la siguiente manera (Tabla 11).

N° Piso	Nº de VLAN
PB	110
Piso 1	111
Piso 2	112
Piso 3	113
Piso 4	114
Piso 5	115
Piso 6	116
Voz	9

Tabla 11. "Relación de VLAN por piso" Fuente: (creación propia, 2014).

Para cada una de estas VLAN se ha considerado una configuración VRRP[39] en la cual, se tendrá 2 direcciones IP físicas y una virtual siendo esta virtual, el gateway o puerta de enlace para cada uno de los segmentos utilizados en el instituto.

También se consideró la creación de VLAN para los segmentos de los servidores en donde se alojan las aplicaciones, estos segmentos de red, en donde se encuentran los servicios de correo electrónico, DNS, SAN[40], directorio activo y demás aplicaciones relevantes para el instituto, tendrán configurado listas de control de acceso (ACL), para brindar mayor seguridad a estos servicios que son vulnerables a ataques tantos internos como externos.

VLAN creadas tanto para red LAN como para red de servidores, administración y de comunicación de equipos (Tabla 12).

[39]**VRRP:**Virtual redundancy router protocol, se utiliza para generar un gateway virtual y dos interfaces fisicas, si una de ellas falla la comunicación no se pierde por el gateway virtual.
[40]**SAN:**Storage area network, es como un disco duro enorme en el cual la red local puede tener acceso a datos como solicitudes, respaldos, etc.

N° Piso	Nº de VLAN	Rango de direccionamiento IP	Mascara de Red	N° direcciones IP para asignar	Tipo de Servicio
PB	110	172.19.0.1 - 172.19.7.254	255.255.248.0	2046	Datos
Piso 1	111	172.19.8.1 - 172.19.15.254	255.255.248.0	2046	Datos
Piso 2	112	172.19.16.1 - 172.19.23.254	255.255.248.0	2046	Datos
Piso 3	113	172.19.24.1 - 172.19.31.254	255.255.248.0	2046	Datos
Piso 4	114	172.19.32.1 - 172.19.39.254	255.255.248.0	2046	Datos
Piso 5	115	172.19.40.1 - 172.19.47.254	255.255.248.0	2046	Datos
Piso 6	116	172.19.48.1 - 172.19.55.254	255.255.248.0	2046	Datos
Prueba	117	172.19.144.1 - 172.19.151.254	255.255.248.0	2046	Datos
PB a 6	9	172.18.0.1 - 172.18.7.254	255.255.248.0	2046	Voz
Admón.	2,5	10.1.1.1 – 10.1.1.254 172.16.37.1 – 172.16.37.254	255.255.255.0	253	Datos

Perfil	Nombre	IP Inicial	Mascara de Red	Puerta de Enlace
Aplicación	Pollux	172.20.51.20	255.255.255.0	172.20.51.1
	Gocos	172.20.52.20		172.20.52.1
	Almeisan	172.20.53.20		172.20.53.1
	Mebsuta	172.20.54.20		172.20.54.1
	Mekbuda	172.20.55.20		172.20.55.1
	Propus	172.20.56.20		172.20.56.1
	Tejat	172.20.57.20		172.20.57.1
	Wasat	172.20.58.20		172.20.58.1
	Alya	172.20.59.20		172.20.59.1
	Unukalhai	172.20.51.20		172.20.51.1
BD SQL	Cujam	172.20.22.20	255.255.255.0	172.20.22.1
	Kornephoros	172.20.23.20		172.20.23.1
	Maasym	172.20.24.20		172.20.24.1
	Rasalgethi	172.20.25.20		172.20.25.1
	Sarin	172.20.61.20		172.20.61.1
Oracle	Antares	172.20.20.20	255.255.255.0	172.20.20.1
Oracle	Beltegeuse	172.20.21.20	255.255.255.0	172.20.21.1
Web	Alhena	172.20.62.20	255.255.255.0	172.20.62.1
	Arneb	172.20.62.21		172.20.62.1
	Nihal	172.20.63.20		172.20.63.1
SAP	Alnair	172.20.50.25	255.255.255.0	172.20.50.1
	Algot	172.20.50.20		
	Atik	172.20.50.21		
	Menkib	172.20.50.22		
	Mirfak	172.20.50.23		
	Achira	172.20.50.24		
	Caph	172.20.31.20		172.20.31.1
	Navi	172.20.31.21		
	Rukbah	172.20.31.22		
	Scheadar	172.20.31.23		
	Tsih	172.20.31.24		

Tabla 12. “Tabla de Direccionamiento IP datos y voz” Fuente: (creación propia, 2014).

Las VLAN y ACL son creadas en el switch core de capa 3 que cuenta con la capacidad de gestionar grandes cantidades de tráfico por ser un equipo robusto, en este switch mantendrá un constante flujo de tráfico, ya que será responsable de la comunicación entre usuarios locales y servicios internos como también usuarios locales y servicio a Internet, este dispositivo será capaz de la comunicación entre las diferentes VLAN.

La implementación de las VLAN en los segmentos de usuarios, servidores y voz, garantiza una mejor distribución y seguridad en la red, permitiendo localizar rápidamente posibles problemas a futuro además de minimizar los dominios de broadcast.

3.5 TECNOLOGÍAS Y HERRAMIENTAS UTILIZADAS

3.5.1 REDES LAN Y VLAN

En las redes LAN todos los grupos de trabajo están en una red, es decir, en un mismo segmento de la red, compartiendo el ancho de banda y dominio de broadcast, dificultando el crecimiento de usuarios y cambios en los miembros del grupo de trabajo, y lo más importante es la limitación geográfica.

Las redes VLAN agrupan a las redes de forma lógica en vez de física lo que permite que los usuarios y grupos de trabajo estén en diferentes ubicaciones geográficas. Al disminuir los usuarios de un mismo grupo lógico distribuidos en diferentes segmentos se aumenta el ancho de banda para el grupo de usuarios. Con los nuevos segmentos se pueden implementar diferentes topologías y protocolos para cada uno, permitiendo el control absoluto del tráfico de entrada y salida de las VLAN hacia otras.

Para grandes institutos y organizaciones el factor más importante, es el rendimiento de la red para la productividad y reputación de la misma. Una de las tecnologías que contribuyen al alto rendimiento de la red es simplemente la

división de los grandes dominios de broadcast en unos más pequeños con la implementación de VLAN. Al hacer que los dominios de broadcast sean más pequeños los dispositivos se dividen en diferentes grupos para mantener el tráfico de cada grupo de manera independiente.

En lugar de tener todos los host conectados, es más práctico y manejable agrupar los equipos en redes específicas. Esta división de la red se les denomina subredes.

Las subredes pueden agruparse en factores como:

***Ubicación geográfica**:* La localización de los host se puede dar en diferentes edificios brindando el mismo servicio.
***Propósito**:* Concentrar en el mismo espacio las actividades en común.
***Propiedad**:* Hacer la diferencia entre los privilegios de los interno-externo y privado-publico.

La siguiente (Fig.38) se muestra los host de recursos humanos en una LAN y ventas en otra LAN, esto funciona sin ningún problema debido a que todos los departamentos están juntos físicamente, por lo que es fácil proporcionales los servicios de la red.

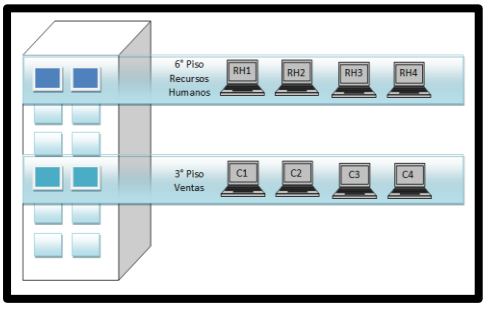

Fig. 38 “Administración de una LAN” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

La organización en la (Fig.39) es la misma con la (Fig.38) pero con la única variante de que los grupos de trabajo de R.H. y de ventas están distribuidos en los cuatro edificios, permaneciendo en el sexto piso recursos humanos y en el tercer piso el de ventas, conforme va creciendo la red es menor su rendimiento y más difícil su administración.

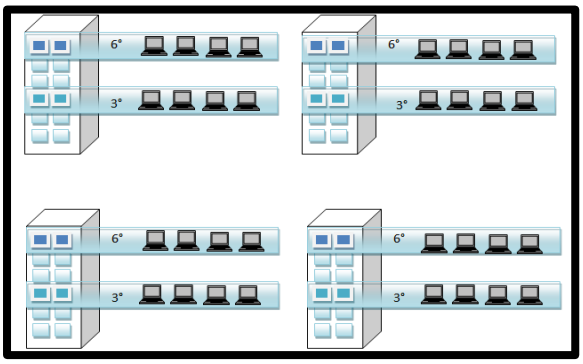

Fig. 39 “Administración de una LAN extensa” Fuente: *CCNA Exploration 4.0, Módulo III, Conmutación y conexión inalámbrica de LAN.*

La solución al crecimiento de las estaciones de trabajo es utilizar una tecnología lógica de red denominada LAN virtual (VLAN), lo que permite a un administrador de la red cree grupos de dispositivos conectados de manera lógica, lo que hace que se comporten como si estuvieran en distintas redes independientes e inclusive compartiendo la infraestructura común con otras VLAN, permitiendo que las redes y subredes múltiples existan en la misma red conmutada.

Cuando se configura una VLAN se puede poner un nombre para describir la función principal de esta estación de trabajo, además implementar políticas de acceso. En los switches se da de alta las VLAN así como indicar su puerto correspondiente. El acceso está dividido en un rango normal o un rango extendido.

3.5.2 VOZ IP

VoIP voz sobre el protocolo de Internet es un método por el cual se toman las señales de audio analógicas (líneas análogas) y se les transforma en datos digitales que pueden ser transmitidos a través de Internet hacia una dirección IP determinada.

La VoIP es un servicio que permite trasmitir voz usando el protocolo IP, es decir tiene la capacidad de trasmitir voz a través de Internet, mantiene una conversación de voz con otra persona usando redes IP en vez de una red de telefonía convencional.[41]

Esto se hace a través de dispositivos de conmutación telefónica IP (Conmutadores IP), que son los aparatos que administran sus líneas convencionales, con el objetivo de ahorrar costos de comunicación.

- Esta tecnología nos permite la administración de llamadas.
- Simplificación de la infraestructura de comunicaciones.

3.5.3 POWER-OVER-ETHERNET (PoE)

La tecnología Power-Over-Ethernet permite suministrar alimentación eléctrica y al mismo tiempo enviar datos a través del mismo cable de la LAN, de este modo reduce la cantidad de cables facilitando la instalación y ahorrando espacio, además se elimina la necesidad de que los dispositivos se encuentren cerca de un contacto eléctrico. La norma que define el estándar PoE es IEEE 802.3af finalizado en el verano de 2003, es el primer estándar internacional de distribución de alimentación a través de una LAN Ethernet, esta tecnología facilita y ahorra espacio para las instalaciones y alimentación de dispositivos.

[41]Servicios en red, Francisco Sivianes Castillo, Gemma Sánchez Antón, Jorge Ropero Rodríguez, etal.

- La instalación no supone gasto de tiempo ni de dinero ya que no es necesario realizar un nuevo cableado.
- Los dispositivos se instalan fácilmente donde es colocado un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación.
- La alimentación a todos los dispositivos PoE conectados se puede garantizar por medio de un UPS conectado a los conmutadores PoE; incluso si se produce un corte del suministro eléctrico, además, los dispositivos se pueden apagar o reiniciar desde un lugar remoto.

3.5.4 STACK

Es la conexión de dos o más dispositivos a través de un puerto propietario del fabricante visualizándose en la red como una sola unidad lógica, para formar un Stack (Fig.40) es necesario que los equipos sean del mismo fabricante.

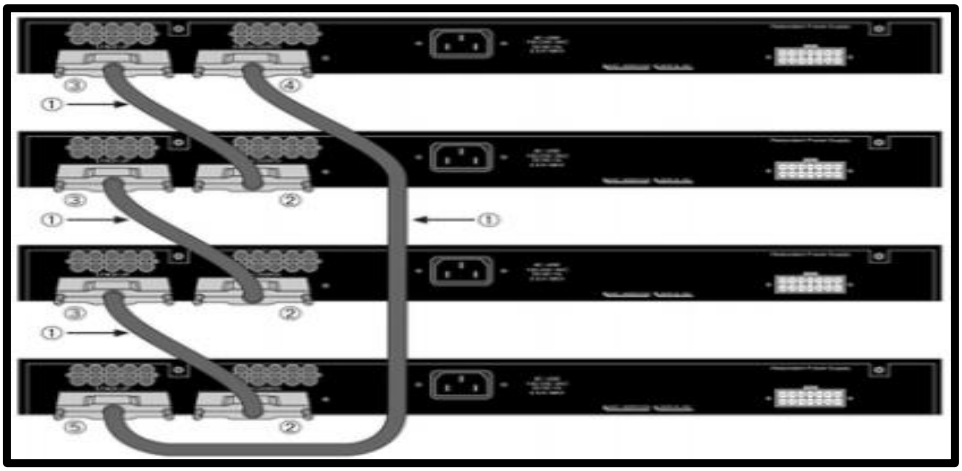

Fig. 40 “Stack” Fuente: *Confuguration guide fastIron , Brocade.*

3.5.5 CLUSTER

El desarrollo de los cluster siempre ha sido a las redes de computadoras, el primer cluster comercial fue el ARCNet, desarrollado en 1977por la corporación DataPoint.[42]

La palabra cluster significa grupo, equipos independientes interconectados que ejecutan una serie de aplicaciones de forma conjunta, este tipo de sistema constituye flexibilidad y gran escalabilidad para aplicaciones que requieren una mayor capacidad de recursos y memoria, para el usuario final aparece como una solo sistema de aplicaciones.

No se tiene una fecha exacta del primer cluster, se otorga que la base científica de este concepto del procesamiento en paralelo la creo Gene Amdahl de IBM en 1967.

Las funciones de los cluster son, además de un alto rendimiento y eficiencia, garantizar que en el momento en que se produzca un fallo en Hardware en alguno de los dispositivos del conjunto, no falle el funcionamiento ni la disponibilidad del sistema informático, porque la operación que se estaba realizando en uno de los dispositivos del cluster puede pasar a realizarla otro[43] miembro, además una característica especial de los sistemas en cluster es que mejora la disponibilidad.

[42]Administración de sistemas operativos en red Miquel Colobran Huguet, Josep María Arqués Soldevila, Eduardo Marco Galindo, Editorial UOC, Primera edición castellana 2008

[43]Seguridad Informática, Alfonso Gracia-Cervigón Hurtado, María del Pilar Alegre Ramos, Ediciones Paraninfo, SA 1ra Edición 2011

CARACTERÍSTICAS

- Un cluster consta de 2 o más nodos conectados entre sí por un canal de comunicación.
- Cada nodo únicamente necesita en elemento de proceso, memoria y una interfaz para comunicarse con la red del cluster.
- Los cluster necesitan Software especializado, ya sea a nivel aplicación o nivel de núcleo.

Todos los elementos del cluster trabajan para cumplir una funcionalidad conjunta, sea la que sea. Es la funcionalidad la que caracteriza el sistema.

SERVICIOS DE LOS CLUSTER

- Alto rendimiento.
- Alta disponibilidad.
- Equilibrio de carga.
- Escalabilidad.

La creación de un cluster permite el balanceo de carga que a su vez distribuye las peticiones entre varios dispositivos de tal forma que todos los servidores respondan al mismo número de peticiones.

CAPÍTULO IV
PRUEBAS

CAPÍTULO IV. PRUEBAS

Esta fase tiene como principal objetivo el lograr la convivencia de la infraestructura actual a la nueva, la cual cuenta con los switches de capa 3 y los switches con tecnología PoE, el cambio debe ser de manera gradual hasta completarse y tener toda la red del instituto con la nueva infraestructura. Ya que no es posible realizar un cambio en el cual la operación se interrumpa por un lapso de tiempo prolongado, debido a que las aplicaciones son consultadas por usuarios externos y deben estar disponibles por ser aplicaciones de consulta pública.

La primera fase es establecer la comunicación entre los switches de capa 3 core MLX y los switches donde se encuentran alojados los servidores y usuarios, por ello, se realizaron pruebas con segmentos de red de baja prioridad asegurando un bajo o nulo impacto a la operación del instituto.

4.1 CONVIVENCIA DE ENTRE CORE CON SEGMENTOS DE RED DE BAJA PRIORIDAD

Esta fase inicial es primordial ya que del éxito de esta prueba depende la migración de todos los segmentos de red donde se encuentran alojados los servidores, que dan servicio a las diferentes aplicaciones alojadas en el instituto.

Para lograr la convivencia entre los switches actuales operando, con los nuevos switches de capa 3 core MLX fue necesario establecer la conectividad entre ambos, aplicado en el punto donde se concentra el tráfico en este caso en particular es el firewall, por ello se configuraron dos interfaces con un segmento de red exclusivo para esta comunicación el cual fue 172.16.37.0/24, se configuraron dos puertos por la alta disponibilidad que cuentan los switches de capa 3 core MLX, la configuración de puertos y rutas estáticas se debe realizar en el cluster de firewall para asegurar lo correcta operación en caso de alguna falla en cualquiera

de los dos equipos. La asignación de direcciones IP en cada uno de los dispositivos se realizó en base a la siguiente (Fig.41).

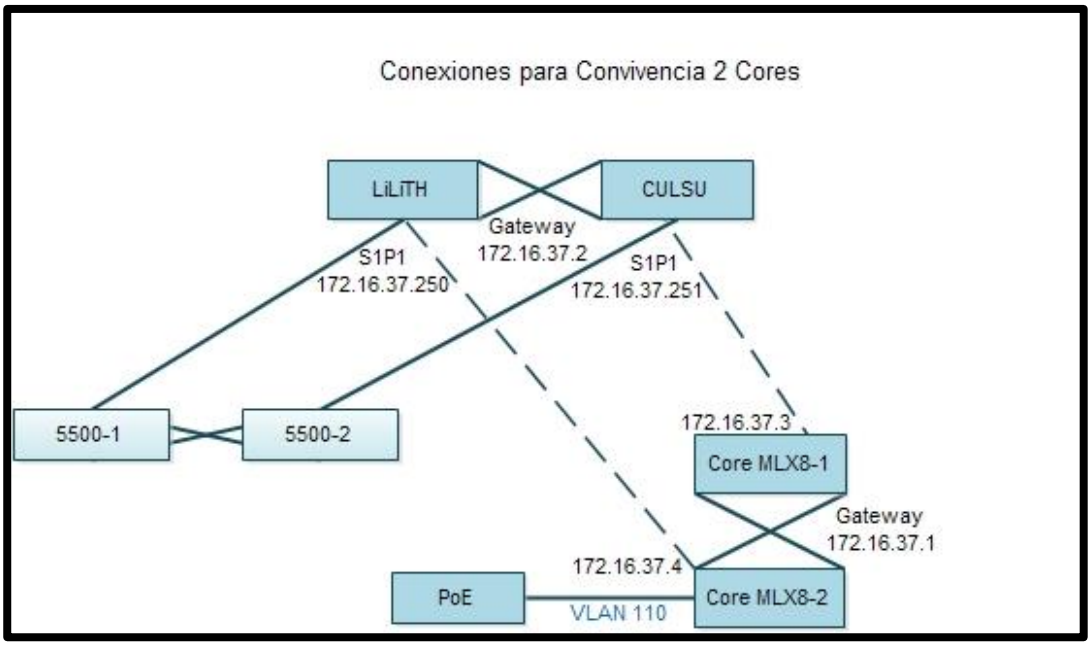

Fig. 41 “Conexiones para Convivencia 2 core” Fuente: (creación propia, 2014).

En el diagrama se muestran las direcciones IP asignadas a cada uno de los equipos así como las direcciones IP virtuales las cuales se consideran gateway de los equipos, estas direcciones IP virtuales nos brindan una redundancia y disponibilidad en la comunicación de los equipos. La configuración de las rutas estáticas en el cluster del firewall para esta etapa de la prueba tiene dos rutas destino, una para los switches de la antigua infraestructura y otra para los switches de capa 3 con los que se pretende realizar la comunicación.

```
default:static:network:172.19.144.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.48.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.40.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.20.64.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.19.24.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.32.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.16.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.8.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.120.0:masklen:21:gateway:address:172.16.37.1
```

```
default:static:network:172.18.0.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.128.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.16.120.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.19.112.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.20.51.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.52.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.53.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.54.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.55.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.57.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.58.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.59.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.60.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.22.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.23.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.24.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.25.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.61.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.20.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.21.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.62.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.63.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.50.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.31.0:masklen:24:gateway:address:172.16.37.1
default:static:network:10.1.1.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.56.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.20.66.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.19.0.0:masklen:21:gateway:address:172.16.37.1
default:static:network:172.16.42.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.44.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.14.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.43.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.32.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.5.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.33.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.35.0:masklen:24:gateway:address:172.16.37.1
default:static:network:172.16.31.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.30.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.29.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.28.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.27.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.26.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.17.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.16.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.15.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.13.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.8.0:masklen:24:gateway:address:172.16.99.2
default:static:network:192.168.124.0:masklen:22:gateway:address:172.16.99.2
default:static:network:172.16.7.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.6.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.10.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.9.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.4.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.3.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.2.0:masklen:24:gateway:address:172.16.99.2
default:static:network:172.16.18.0:masklen:24:gateway:address:172.16.99.2
```

Las dirección IP destino o gateway de las rutas estáticas 172.16.99.2 y 172.16.37.1 corresponden a los anteriores switches que tienen conectados los servidores en operación y los switches de capa 3 core MLX respectivamente, estas rutas estáticas nos indican que segmentos de red están conectados en cada uno de los switches, en esta fase se debe garantizar la comunicación del segmento de red de los servidores que se encuentran alojados en la infraestructura actual, con los segmento de red de los usuarios alojados en la infraestructura a implementar.

4.2 MIGRACIÓN DE SEGMENTOS DE RED DE DATOS Y VOZ

En la migración de los segmentos de red correspondientes a los usuarios no fue necesario realizar pruebas debido a que esta migración se realizo en una sola exhibición, instalando los nuevos switches con la característica PoE para la utilización de la tecnología VozIP, esto se realizó en cada uno de los 6 IDF que cuenta el instituto, desconectando y conectando los patch cords de cada uno de los pisos.

La fase de pruebas para la instalación de los teléfonos IP fue en primera instancia, configurando en cada uno de ellos direcciones IP estáticas para verificar su correcto funcionamiento, esta configuración se dejó por un periodo temporal para asegurar su correcto funcionamiento. La siguiente etapa en la instalación de los teléfonos IP fue la asignación de direcciones IP dinámicas configurando en cada uno de los teléfonos la VLAN de voz, la asignación de direcciones IP dinámicas es posible debido a un servidor DHCP en cual se encuentra alojado en el conmutador[44].

[44]**Conmutador:** solución de telefonía, que se refiere a un equipo central (mejor conocido como central telefónica) el cual concentra líneas telefónicas, extensiones telefónicas y servicios de comunicación para permitir, que usuarios internos se comuniquen entre sí y compartir líneas telefónicas con propósitos de recibir o de generar llamadas desde y hacia el exterior de la organización.

4.3 PRUEBAS DE CONECTIVIDAD

Estas pruebas tienen la función de asegurar una correcta comunicación entre las infraestructuras actuales y nuevas, el primer paso fue establecer la comunicación de redes de bajo impacto operacional o de pruebas, una vez garantizando estas pruebas se inició una fase de migración de servicios como DHCP, streaming, correo electrónico, telefonía, directorio activo, etc. Esta migración contó con varias etapas previas como la identificación de cableado, revisión de configuraciones en tarjetas de red de cada uno de los servidores para asegurar el funcionamiento de todas las aplicaciones y servicios que se encontraban operando en la infraestructura anterior.

La primer prueba básica de comunicación fue con el protocolo ICMP[45] con el cual se garantiza la disponibilidad de los equipos y posibles errores en la comunicación, esta prueba aunque es muy simple nos da la seguridad de la comunicación de los equipos. Otra de las pruebas que se consideró es la revisión de velocidades en los puertos a los que trabaja cada interface, una ventaja que nos ofrece la actualización de la red es que al actualizar los equipos de comunicación por ende se refleja en el aumento en la velocidad de las interfaces, ya que debido a que se contaban con equipos obsoletos la máxima velocidad de algunos de los equipos de comunicaciones era de 100Mbps, reduciendo la capacidad de transmisión de datos reflejado en el tiempo de respuesta que percibe el usuario final.

En la actualidad los equipos de comunicaciones tienen un mínimo de 1000Mbps aumentando considerablemente la velocidad de transferencia, esta velocidad se reflejará siempre y cuando se utilicen como mínimo 1000Mbps en interfaces de todos los equipos de comunicación (Fig.42).

[45]**ICMP:** Protocolo de Mensajes de Control de Internet (por sus siglas en inglés de ***I**nternet **C**ontrol **M**essage **P**rotocol*), se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

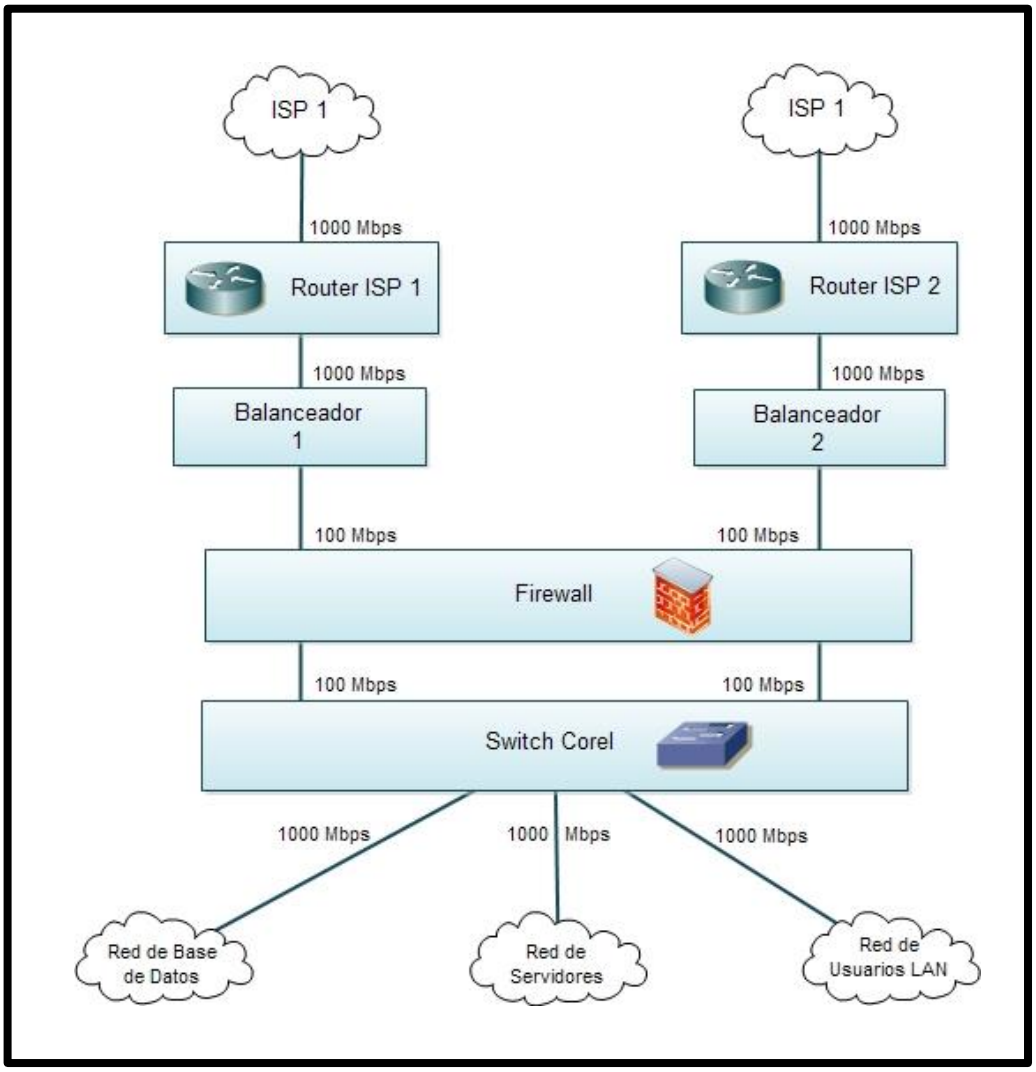

Fig. 42 “Lan a diferentes velocidades” Fuente: (creación propia, 2014).

En el diagrama se observa que la red LAN opera con diferentes velocidades en los equipos de comunicaciones, esto repercute directamente en la velocidad de transferencia ya que sin importar lo actualizados que estén algunos equipos, si uno de ellos no trabaja a la misma velocidad el desempeño de la red se fija a la velocidad del dispositivo más lento, teniendo un deficiente diseño en la red.

Dentro de la etapa de pruebas se realizaron varias actividades previas como los permisos en el equipo de seguridad firewall, que consistieron en dar de alta los segmentos de red que en un principio eran las redes de bajo impacto, pero conforme fue avanzando esta etapa de pruebas se añadieron las redes restantes las cuales contienen los servicios y aplicaciones del instituto, también se tomó en cuenta los permisos de salida hacia la red de Internet, los cuales se fueron actualizando dependiendo de las peticiones de la red de usuarios, fue el mismo caso para los servicios. Todo proceso de migración deberá ser paulatino con ventanas de mantenimiento programadas, teniendo como resultado control de los cambios aplicados.

La implementación de las listas de control de acceso (ACL) requiere una fase de pruebas la cual se aplicó a una red de usuarios que tiene poca concurrencia:

```
access-list 105 permit tcp 172.19.120.0 0.0.7.255 any eq http log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 any eq smtp log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 any eq pop3 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 any eq ssl log
access-list 105 permit icmp 172.19.120.0 0.0.7.255 any any-icmp-type log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq kerberos log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq loc-srv log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 range 137
netbios-ssn log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq ldap log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq microsoft-ds
log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 464 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 636 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 5722 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 range 3268
3269 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 192.168.127.103 range 49152
65535 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq dns log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq ntp log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq kerberos log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq loc-srv log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 range netbios-
ns netbios-ssn log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 389 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 464 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 636 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 eq 5722 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 range 3268
3269 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 192.168.127.103 range 49152
65535 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq kerberos log
```

```
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq loc-srv log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 range 137
netbios-ssn log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq ldap log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq microsoft-ds
log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 464 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 636 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 5722 log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 range 3268  3269
log
access-list 105 permit tcp 172.19.120.0 0.0.7.255 host 172.16.33.71 range 49152  65535
log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq dns log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq kerberos log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq ntp log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq loc-srv log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 range netbios-ns
netbios-ssn log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 389 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 464 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 636 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 eq 5722 log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 range 3268  3269
log
access-list 105 permit udp 172.19.120.0 0.0.7.255 host 172.16.33.71 range 49152  65535
log
access-list 105 deny ip any any
```

Terminada esta prueba, se deberá aplicar las ACL no en el equipo, sino en la *interfaces ve* creadas, que corresponden a los segmentos de red, estas ACL serán aplicadas a la salida de la interfaz permitiendo, dar de alta solamente el servidor y puerto, esto se realizó para una administración más fácil ya que de lo contrario con ACL aplicadas a la entrada de la interfaz, se tendría que dar de alta cada usuario en la ACL para el acceso a un servicio aumentando el archivo de configuración.

Para la asignación de permisos hacia un usuario en particular a un servidor en una ACL, se deberá tener en consideración el servicio DHCP y su respectiva reserva de la dirección IP de dicho usuario, siendo necesaria una etapa de reserva de direcciones IP de los usuarios con permisos hacia algún servidor dentro y/o fuera de la red local, para así asegurar que la dirección IP del usuario será la misma durante el tiempo que tenga vigencia el permiso.

La fase de pruebas concluye al migrar todos los servicios alojados en los anteriores switches a los nuevos switches de capa 2 y 3 de brocade, con esta

etapa terminada se dejarán de utilizar diversos segmentos de red y se retirarán todas las rutas asociadas hacia el destino de los switches de la infraestructura anterior, quedando la red del instituto como se muestra la siguiente (Fig. 43).

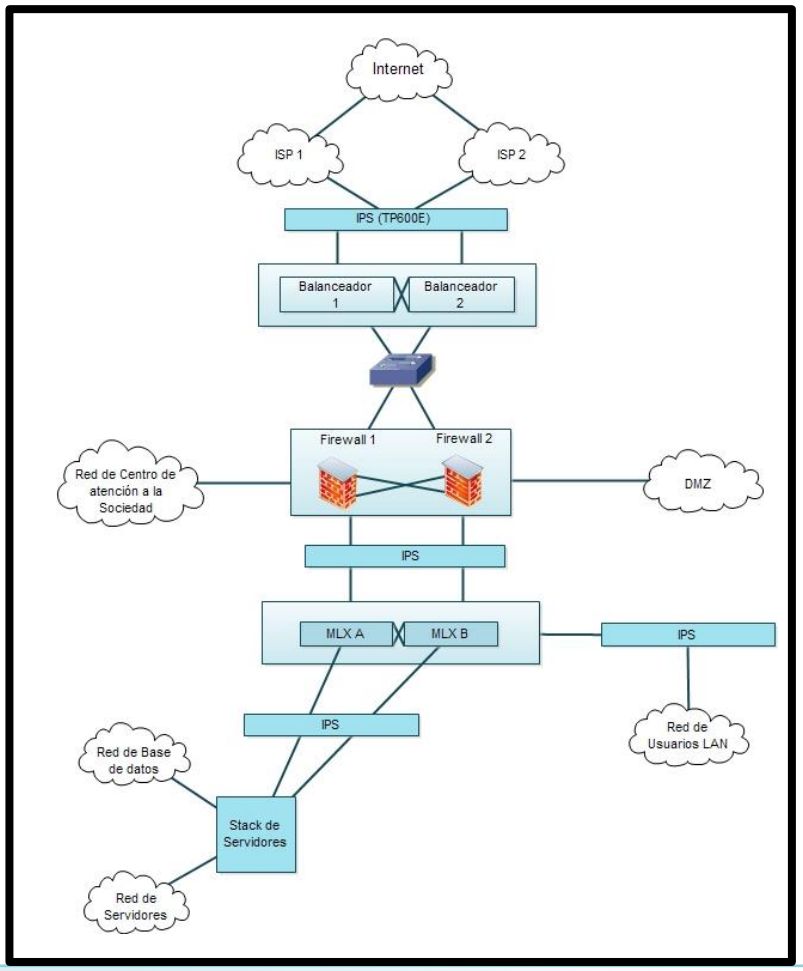

Fig. 43 “Red con Switch Core” Fuente: (creación propia, 2014).

Una vez terminada la migración de los servicios de la infraestructura anterior, será necesaria una depuración y actualización de configuración de rutas estáticas creadas tanto en los switches de capa 3, como en los dispositivos de seguridad siendo éste el firewall, esto con el fin de tener una configuración actualizada y ordenada para mantener una mejor administración.

CAPÍTULO V
IMPLEMENTACIÓN
DE LA NUEVA RED DE ÁREA LOCAL

CAPÍTULO V. IMPLEMENTACIÓN DE LA NUEVA RED DE ÁREA LOCAL

En esta etapa es indispensable realizar la migración por partes ya que el instituto cuenta con aplicaciones en operación que son críticas y no es posible tenerlas por periodos largos fuera de servicio. Para una primera etapa es indispensable integrar los switches que se instalaran dependiendo del rol que desempeñarán en la capa de acceso, distribución y núcleo.

Una de las primeras tareas previas a la instalación, es identificar el rol que tomarán los switches de las capas de distribución y núcleo, estos switces pueden tener previamente configurado las VLAN para cada uno de los pisos, antes de ser instalados, con el objetivo de realizar la migración de los usuarios a los nuevos switches de la capa de acceso de la nueva infraestructura y concediendo un periodo de estabilidad en la red de usuarios, para proceder a migrar la red de los servidores y completar la fase de migración (Fig.44).

VLAN 172.20.X.X / 24	**Servicios a Usuarios Internos**  Correo Electrónico NAS DC Chat
VLAN 172.20.X.X / 24	**Bases de Datos**  Oracle MsSQL
VLAN 172.20.X.X / 24	**Aplicaciones**  POT Informex
VLAN 172.20.X.X / 24	**Soporte**  Consolas WS
VLAN 172.20.X.X / 24	**QA y Desarrollo**  Des QA Des QA Oracle
VLAN 172.20.X.X / 24	**Respaldos**  BCK Data domain Nic svr

Fig. 44 “Servicios” Fuente: (creación propia 2014).

5.1 INSTALACIÓN

Esta etapa consta de la instalación física de los nuevos equipos a utilizar, en la instalación de los switches de la capa de acceso que se diferencian de los demás por tener la funcionalidad de operar con tecnología PoE, función necesaria para poder brindar servicio de voz a través de teléfonos IP, por medio de una VLAN diferente a la de servicio de datos, otorgando calidad de servicio y disponibilidad.

Se planteó un direccionamiento lógico que ayuda a la identificación del servicio y a reducir los dominios de broadcast, los cuales en ambientes con gran cantidad de equipos son responsables de la perdida de datos y la falta de disponibilidad en una red local.

La instalación de los switches de capa 3 es más compleja debido a la configuración y tamaño de los mismos, ya que se deberá plantear el espacio a

ocupar y el suministro de energía al cual se conectará y debido a que son equipos de operación crítica, se tendrá que considerar una fuente de respaldo de enegia eléctrica por posibles fallas a futuro. Las actividades previas a la puesta en marcha constan de configurar previamente VLAN, rutas estáticas, listas de acceso y modos de puertos, que previamente se analizó con la red de la anterior infraestructura, teniendo especial atención a la red de servidores, ya en estas redes se deberá considerar los permisos que tienen configurados a la entrada y salida para poder migrar la red lo más transparente posible, sin afectación en los servicios hacia los usuarios locales y externos.

Otro asunto de suma importancia, es el cableado estructurado ya que es el medio responsable de la transmisión de datos y un error en este afectaría a una parte de la red local e incluso a toda. No importando la tecnología aplicada en los switches es necesario considerar cotizar la compra de buen material para la instalación de cableado, tanto horizontal como vertical ya que un ahorro en este aspecto además de que causaría falta de disponibilidad en la red local, se generaría un costo adicional en el reemplazo del mismo. En este proyecto se tomará en cuenta la ya existencia de la infraestructura de comunicación como el cableado vertical entre cada uno de los pisos y el cableado horizontal en cada piso.

El primer cambio a realizar es la instalación y cambio de los switches de la capa de acceso con la característica de tener la tecnología PoE, previamente configurando las VLAN perteneciente de cada piso, en este paso se debe de tener especial cuidado en la comunicación de los switches de la capa de acceso con los switches de la capa de distribución-núcleo, por ello, se consideró la comunicación a través del medio de fibra óptica para asegurar un mejor y más rápido flujo de datos entre usuarios y aplicaciones e Internet.

Diagrama de conexión entre pisos y core MLX (switch de capa 3) (Fig.45).

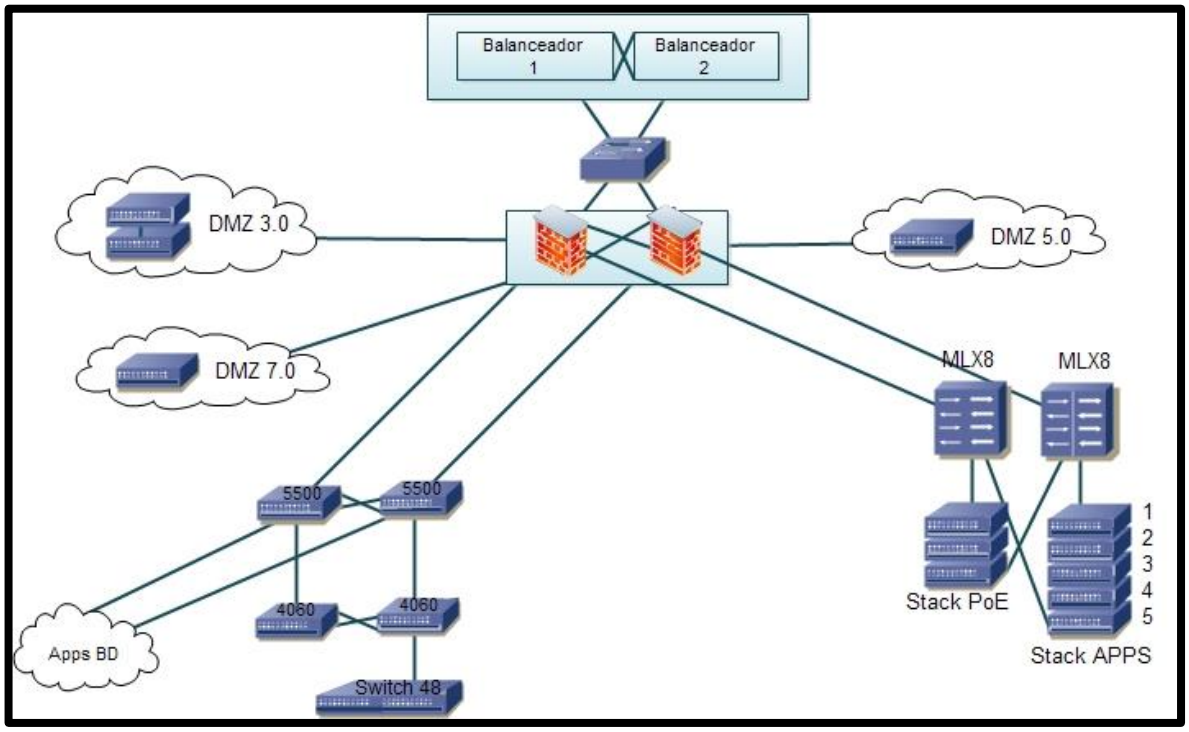

Fig. 45 “Diagrama de Conexión” Fuente: (creación propia, 2014).

Para la instalación de los switches de la capa de acceso, resta la instalación de los switches de capa 3, parte importante debido a que en estos equipos alojarán las redes de servidores y de usuarios, estos equipos de capa 3 son responsables de gestionar todo el tráfico tanto interno como el tráfico saliente, por ser equipos de alta criticidad deberán tener enlaces redundantes para la conexión con los IDF de capa piso, además, de tener en cuenta posibles configuraciones de agregado de enlaces para cuyos servidores requieran un mayor ancho de banda para su optima operación.

Para finalizar la fase de instalación de los switches de la capa de acceso, resta realizar la configuración e instalación de los teléfonos IP para los usuarios, para ello es necesario configurar y propagar la VLAN en el stack de switches de cada piso. Para que cada teléfono IP funcione de manera correcta existen dos opciones

a configurar, la primera es que cada teléfono IP sea configurado con una dirección IP estática o la segunda opción que es la implementación de un servidor DHCP, el cual otorgue de un pool de direccionamiento IP las direcciones a cada uno de los teléfonos IP, para ello bastará indicar en cada uno de los teléfonos el ID de VLAN destinada para el servicio de voz, la cual tendrá el direccionamiento asignado establecido en la configuración de dicha VLAN, cabe aclarar que para este proyecto solo se enfocará en la segmentación del servicio de voz IP mediante una VLAN la cual garantizará calidad de servicio y disponibilidad, no así en la implementación de un servidor DHCP.

Para garantizar la comunicación de los diversos segmentos de red, las VLAN de voz y de datos deberán ser propagadas en los puertos destinados en modo trunk o modo lag para los switches de capa 3 y modo tagged y link aggregation en los switches de acceso, estos modos de puerto permite el tráfico de más de una VLAN aceptando la comunicación de diferentes segmentos de red en una misma red de área local.

Comunicación de diferentes VLAN (datos y voz) (Fig.46).

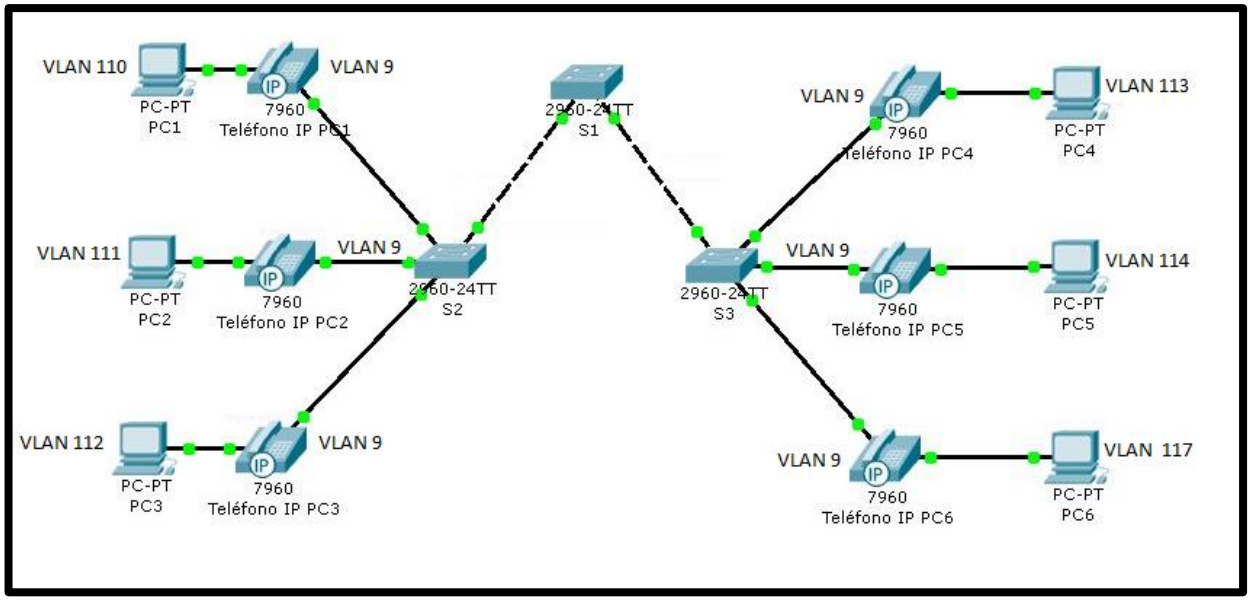

Fig. 46 “VLAN voz y datos” Fuente: (creación propia, 2014).

5.2 CONFIGURACIONES

La implementación de la actualización de una red local plana a una red local segura, segmentada con los servicios de voz y datos recae en gran parte en las configuraciones de VLAN, pero no solo estas configuraciones son necesarias para la correcta operación de la red local, ya que también depende de la seguridad a implementar en cada una de las redes y las velocidades de configuración en los puertos que tendrán la función de modo tagged.

.

Una de las primeras acciones es la configuración de los puertos en cada uno de los switches, tanto de acceso como en los de núcleo-colapsado, para lo cual se determinará que puertos tendrán una configuración en modo acceso (untagged) permitiendo una sola VLAN y que puertos tendrán una configuración en modo trunk (tagged) el cual permite el tráfico de más de una VLAN en una interface.

Una de las primeras configuraciones que se realizó tanto en los switches de acceso como en los switches core fue la creación de VLAN, estas VLAN corresponden con la relación en la (Tabla 12) donde se muestran las VLAN creadas, tanto para red datos y telefonía, como para red de servidores y de administración de los dispositivos.

Ya definidas el nombre y el direccionamiento de cada una de las VLAN los comandos para la creación de las mismas son los siguientes:

5.2.1 CONFIGURACIÓN DE VLAN PARA SWITCHES CORE

Ingresar a los equipos en modo configuración:

```
Stack_Piso1#configure terminal
Stack_Piso1(config)#
```

La creación de las VLAN es una configuración básica para la segmentación de la red local, ya que estas VLAN identificarán los segmentos, por ello es necesario

nombrar estas VLAN creadas, así como asignar los modos de troncales o de acceso de cada VLAN

```
Stack_Piso1(config)#
Stack_Piso1(config)# vlan "Número representativo de la VLAN"
Stack_Piso1(config-vlan-2)# name "Nombre distintivo de la vlan a crear"
```

Seleccionar el modo de los puertos para su comunicación tagged o untagged

```
Stack_Piso1(config-vlan-"No")# tagged ethernet stackID/slot/port
Stack_Piso1(config-vlan-"No")# untagged ethernet stackID/slot/port
```

5.2.2 COMUNICACIÓN INTER-VLAN

Esta comunicación es indispensable ya que es la responsable de la comunicación entre VLAN, esta característica solo es configurable en equipos de capa 3 del modelo OSI, en equipos brocade recibe el nombre de *virtual routing interfaces* la cual es una interface virtual de ruteo que los switches de capa 3 brocade usan para enrutar tráfico entre VLAN, por ello es necesario configurar un virtual routing interfaces (ve) para cada una de las VLAN creadas, asignando una dirección IP correspondiendo ésta, a la puerta de enlace para cada VLAN creada.

```
MLX_1(config)# vlan 20
MLX_1(config-vlan-20)# untagged ethernet stackID/slot/port
MLX_1(config-vlan-20)# tagged ethernet stackID/slot/port
MLX_1(config-vlan-20)# router-interface ve 20
MLX_1(config-vlan-20)# interface ve 20
MLX_1(config-vif-20)# ip address 172.20.20.1/24
```

Configuraciones de switches core (núcleo colapsado) ver anexo 1

5.2.3 CONFIGURACIÓN DE VLAN PARA SWITCHES DE PISOS

La configuración de VLAN en los switches de capa de acceso los cuales cuentan con la funcionalidad de PoE, es idéntica a la configuración en los switches de capa 3. La diferencia entre la configuración de uno y otro switch, es que en los switches

de capa de acceso solo se activarán las VLAN más no se realizará un proceso de ruteo.

La configuración de cada stack de switches por piso se diferencia en la activación de su VLAN, habilitando en todos los stack de piso las VLAN de administración, de voz, de pruebas y de redes inalámbricas si fuese el caso, pero no así de la VLAN correspondiente al piso de cada stack de switches. Para la creación de VLAN se deberá ingresar en modo configuración global:

```
Stack_Piso1(config)#
Stack_Piso1(config)# vlan "Número representativo de la VLAN"
Stack_Piso1(config-vlan-2)# name "Nombre distintivo de la vlan a crear"
```

Seleccionar el modo de los puertos para su comunicación tagged o untagged

```
Stack_Piso1(config-vlan-"No")# tagged ethernet stackID/slot/port
Stack_Piso1(config-vlan-"No")# untagged ethernet stackID/slot/port
```

Para la configuración de las VLAN de cada piso se debe habilitar el modo tagged o troncal en los puertos que contendrán las VLAN de datos y de voz de cada piso que estarán conectados a los dispositivos finales, también se deberá considerar el modo tagged a los puertos que tendrán conexión con los switches core de capa 3.

Creadas las VLAN es necesario configurar los switches de cada piso, a la vez de indicar que puertos trabajarán con una VLAN de voz y de datos simultáneamente. Con el comando *dual-mode* que permite el tráfico de datos tagged y untagged en un solo puerto.

La configuración de enlaces troncales, los cuales se comunicarán con los switches de capa 3 por medio de fibra óptica, tienen una configuración de link aggregation la cual proporciona un aumento de ancho de banda y redundancia en los enlaces, otorgando caminos alternos si alguno de estos falla, es importante indicar que una interfaz configurada con el comando tagged, solo permitirá el tráfico de paquetes

(con un ID de una VLAN). Otro parámetro que se deberá indicar es la cantidad de voltaje que será suministrado en cada puerto PoE.

Configuración PoE de switches capa de Acceso

Esta configuración varía según la marca que se utilice, en algunos equipos se configura manualmente o automáticamente y los modelos más recientes operan con dos estándares, el original 802.3af el cual puede proporcionar hasta 15.4W y el actualizado que puede llegar a proporcionar hasta 25.5W. Para los switches brocade la función PoE se habilita manualmente especificando el estándar a ocupar y permitiendo en el puerto, las VLAN de datos y de voz desde la interface de línea de comando como se muestra:

Los comandos que se utilizaron en la configuración de los puertos son los siguientes y se ejemplificará con la configuración del piso 2.

Ingresar al stack del piso en modo configuración global

```
Stack_Piso1(config)#
```

Ingresar ya sea por puerto o por un grupo de puertos a las interfaces Ethernet por puerto:

```
Stack_Piso1(config)# interface ethernet stackID/slot/port
Stack_Piso1(config-if-e1000-stackID/slot/port)#dual-mode 112
Stack_Piso1(config-if-e1000-stackID/slot/port)# inline power power-limit
15400
```

El comando `dual-mode 112` especifica la VLAN 112, como la VLAN por default la cual se caracteriza por permitir trafico untagged, se realizará esta configuración en todos los switches de cada piso, variando solamente el ID de VLAN, el comando dual mode permite el trafico tagged, configurado para los servicios de voz y datos que se transmitirán en un solo puerto.

El comando `inline power power-limit 15400` se utiliza para habilitar el modo PoE que brinda corriente eléctrica a través del puerto, permitiendo así que un teléfono

IP funcione sin necesidad de conectarlo a una toma de corriente eléctrica este comando, se regula en base a la norma IEEE 802.3af.

La configuración se puede realizar de manera grupal aplicando los mismos comandos de configuración, pero seleccionando más de un puerto, como se muestra:

```
Stack_Piso1(config)#interface ethernet stackID/slot/port to stackID/slot/port
Stack_Piso1(config-if-e1000-stackID/slot/port-stackID/slot/port)#dual-mode 112
Stack_Piso1(config-if-e1000-stackID/slot/port-stackID/slot/port)#inline power power-limit 15400
```

Las configuraciones de los stack de cada piso. Ver anexo 2

5.3 CONFIGURACIÓN DE STACK

La configuración stack en los switches brocade tienen diferentes beneficios como; la administración de todo el stack por una sola dirección IP, soporta hasta ocho unidades por stack, consta de dos configuraciones posibles lineal y anillo siendo la configuración anillo, la más recomendada por tener mejor redundancia, esta configuración tiene la característica de mantener un miembro activo, el cual administra todo el stack y un miembro de respaldo, el cual tiene total redundancia con el miembro activo si éste llegase a fallar. La configuración se puede realizar de tres maneras diferentes; instalación segura, automática y manual.

Sin embargo la configuración utilizada fue la instalación automática, con una topología de stack tipo anillo, los switches brocade determinan los candidatos a ser parte del stack en base a un puerto específico, el cual cuenta con características para la asociación al stack, para considerar un equipo a ser candidato a ser parte del stack es necesario que su configuración este limpia, es decir, que el dispositivo tenga la configuración de fabrica, excepto en el dispositivo que tendrá la función de activo. Configuración de Stack (Fig.47).

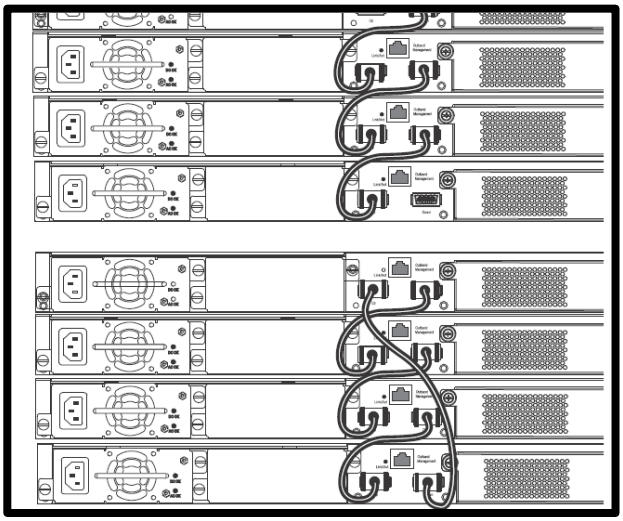

Fig. 47 “Configuración de Stack “ Fuente: *Confuguration guide fastIron , Brocade.*

Los pasos a seguir para la configuración de stack son los siguientes:

1. Encender los equipos que se considerarán parte del stack.
2. Asegurarse que todos los equipos excepto el activo no contengan configuración guardada. Para limpiar la configuración de un equipo bastará con ingresar el comando *erase startup-config* y reiniciar el equipo.
3. Ingresar al equipo que fungirá como el miembro activo.
4. Configurar el resto de los dispositivos conectados en stack, asignando un ID diferente a cada uno; del 1 al 8.

```
Switch_Piso1# config t
Switch_Piso1(config)# stack unit 2
Switch_Piso1(config-unit-2)# module 1 fls-24-port-copper-base-module
Switch_Piso1(config-unit-2)# module 2 fls-xfp-1-port-10g-module
Switch_Piso1(config-unit-2)# module 3 fls-xfp-1-port-10g-module
Switch_Piso1(config-unit-2)# stack unit 3
Switch_Piso1(config-unit-3)# module 1 fls-24-port-copper-base-module
Switch_Piso1(config-unit-3)# module 2 fls-xfp-1-port-10g-module
Switch_Piso1(config-unit-3)# module 3 fls-xfp-1-port-10g-module
```

Una parte sumamente importante de la configuración es la asignación de prioridades tanto del miembro activo como del pasivo, el número de la prioridad tiene un rango de 0-255 y en cuanto más grande, mayor prioridad tendrá:

Asignación de prioridad al miembro activo

```
Switch_Piso1# config t
Switch_Piso1(config)# stack unit 1
Switch_Piso1(config-stack-1)# priority 255
```

Asignación de prioridad al miembro pasivo

```
Switch_Piso1# config t
Switch_Piso1(config)# stack unit 2
Switch_Piso1(config-unit-2)# priority 240
```

Para concluir con la configuración del stack solo restaría guardar la configuración con el comando:

```
Switch_Piso1#write memory
```

Y habilitar la característica de stack en el switch activo con las siguientes líneas:

```
Switch_Piso1# config t
Switch_Piso1(config)#stack enable
```

5.4 MODO TAGGED Y UNTAGGED

Las configuraciones de estas modalidades sobre los puertos, tienen especial importancia ya que sin ellas el flujo de las VLAN no sería posible, ocasionando la no segmentación de una red de área local (LAN). Estas modalidades es un estándar que trabajan todos los switches, sin embargo, en algunos casos se nombran de diferente manera, el modo tagged o trunk es capaz de permitir el tráfico de más de una VLAN por lo tanto es el canal donde fluyen y se comunican las diferentes VLAN creadas, en cambio el modo untagged o acceso permite el tráfico de una sola VLAN especificada en el puerto, por ello es necesario realizar estas configuraciones en toda red a segmentar.

```
Stack_Piso1(config-vlan-"No")# tagged ethernet stackID/slot/port
Stack_Piso1(config-vlan-"No")# untagged ethernet stackID/slot/port
```

5.5 CONFIGURACIÓN DE VRRP

Este protocolo tiene la capacidad de aumentar la disponibilidad de la puerta de enlace dentro de una red local, este aumento de disponibilidad se consigue configurando una interface virtual en vez utilizar equipo físico. La configuración VRRP en este proyecto se basó con el protocolo VRRPE propietario de brocade que supera las limitantes del protocolo anterior, permitiendo configurar prioridades a cada uno de los miembros y en base a la prioridad más alta se asignará la unidad master o activo responsable del enrutamiento del tráfico, otra configuración a realizar es la asignación de VRID que es un identificador de la subred a crear, pero sin duda, la diferencia más importante entre VRRP y VRRPE es que no asigna un equipo como activo o master por default, eliminando esta característica del protocolo.

Para la implementación de esta configuración en la red local es necesario contar con switches de marca brocade, basándonos en los dos switches de capa 3 y configurándoles una interface virtual para cada segmento creado, el tráfico se

enrutará solo por uno de los dos switches, este enrutamiento se basa en la prioridad que se le asignará al switch que tomará el rol de master o activo (Fig.48).

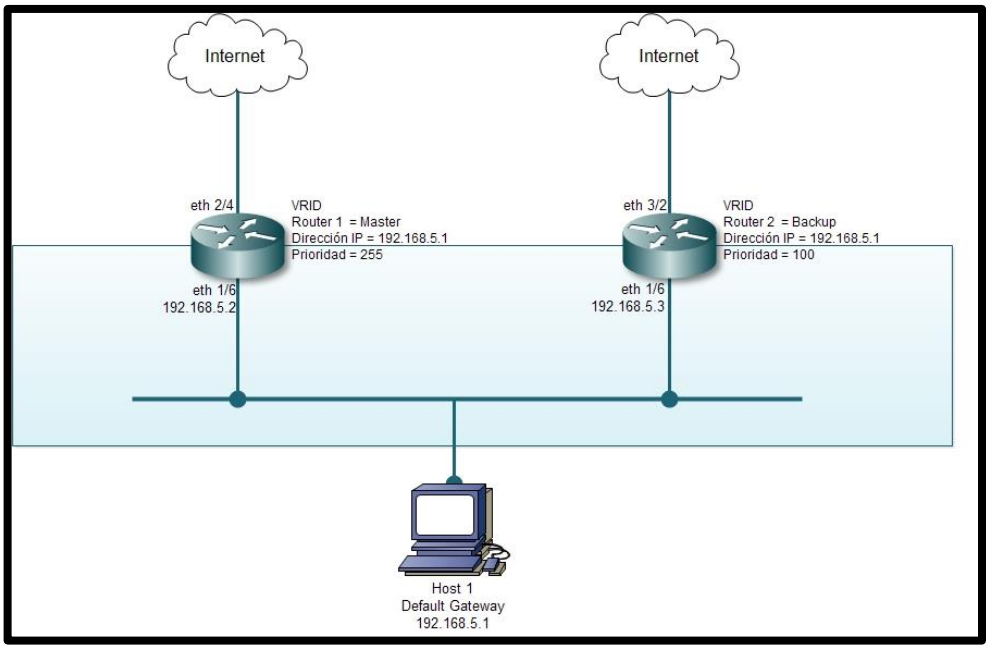

Fig. 48 “Configuracion VRRP” Fuente: (creación propia, 2014).

La configuración que se realizó es la siguiente:

Configuración para el equipo master

```
MLX_A#configure terminal
MLX_A(config)#interface ve 113
MLX_A(config-vif-113)#router vrrp-extended
MLX_A(config-vif-113)#ip vrrp-extended vrid 113
MLX_A(config-vif-113-vrid-113)#backup 255
MLX_A(config-vif-113-vrid-113)#ip-address 172.19.24.1
MLX_A(config-vif-113-vrid-113)#activate
```

Configuración para el equipo de respaldo

```
MLX_B#configure terminal
MLX_B(config)#interface ve 113
MLX_B(config-vif-113)#router vrrp-extended
MLX_B(config-vif-113)#ip vrrp-extended vrid 113
MLX_B(config-vif-113-vrid-113)#backup
MLX_B(config-vif-113-vrid-113)#ip-address 172.19.24.1
MLX_B(config-vif-113-vrid-113)#activate
```

La limitante para este protocolo VRRPE es que solamente funciona entre dispositivos de capa 3 de marca brocade.

El protocolo VRRP es capaz de proveer redundancia en las puertas de enlace dentro de una red LAN, permitiendo rutas alternas sin cambiar la dirección IP o MAC que el host conoce como gateway y que es responsable de la comunicación hacia otros segmentos.

Para el proyecto desarrollado fue necesario duplicar la configuración en los dos switches core, cuyas tareas se centrarán es las capas de núcleo y distribución. La habilitación del protocolo VRRP se realizó en los dos switches core MLX con el siguiente comando:

```
MLX(config)#router vrrp-extended
```

Se deberá crear una interfaz virtual por cada segmento creado, para ejemplificar se tomará como base la configuración del piso 1 en el equipo switch core MLX A.

```
interface ve 111
 ip address 172.19.8.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 111
  backup priority 255
  ip-address 172.19.8.1
  activate
```

```
interface ve 111
```

Comando de configuración, el cual se ingresa a la interfaz virtual asignada a la vlan 111

```
ip address 172.19.8.2/21
```

Comando que permite asignar una dirección IP dentro del comando *interface ve 111* al equipo core MLX A perteneciente al segmento de la vlan del piso 1, se deberá especificar tanto la dirección IP como la máscara de red.

```
ip helper-address 172.20.52.26
```

Comando opcional que permite la comunicación con un servidor DHCP, que otorga direccionamiento lógico de manera automática al segmento que se ha especificado en la VLAN.

```
ip vrrp-extended vrid 111
```

Comando necesario para identificar con un ID el segmento en el cual se configurará el protocolo VRRP

```
backup priority 255
```

Comando que establece dentro del comando *ip vrrp-extended vrid 111* la prioridad del equipo y que en base a esta prioridad tomará el rol de master o backup, prioridad máxima 255, por default 100.

```
ip-address 172.19.8.1
```

Comando que establece la dirección IP de la puerta de enlace que permitirá la comunicación de los equipos conectados de este segmento a otro.

```
activate
```

Comando que habilita la función del protocolo VRRP

Estas líneas de comandos deberán ser realizadas por cada VLAN creada y en cada uno de los equipos switch core MLX diferenciándose en el número de VLAN, ACL aplicada en la interfaz según sea el caso, la prioridad y dirección IP que se deberá asignar en cada uno de los switches core MLX. **Ver anexo número 3**

5.6 CLUSTER DE EQUIPOS

Existen varias configuraciones de cluster en esta red LAN local debido a la alta disponibilidad en los firewall, balanceadores y switches de capa 3, se mostrarán las configuraciones realizadas en estos switches que son responsables de la mayor cantidad de tráfico, que reside en la navegación de los usuarios y servidores, el cluster formado para los switches de capa 3 se realizó mediante el Link Aggregation trunk, el cual provee un nivel de redundancia e incrementa la capacidad de conexión entre los dispositivos de red, que aunado a una configuración de MCT(Multi Chassis Trunking) en el cual se agregan los miembros o enlaces troncales y el ICL (Inter Chassis link) el cual es el enlace de datos para la comunicación entre los equipos del cluster, estas configuraciones garantizan que si un miembro del cluster (MCT) falla, el tráfico de datos conocerá una ruta por medio de la comunicación ICL hacia el otro miembro (MCT), obteniendo así un aumento en la recuperación y rendimiento de la red.

La configuración para el cluster de los switches de capa 3 fue la siguiente:

1. Crear y nombrar el cluster entre los switches core MLX con el comando `cluster "nombre" "asociar un ID"`.
2. Asociar con el comando `rbridge-id` un "ID" para cada equipo en cluster para la su intercomunicación.
3. Creación de la VLAN que usa el cluster para operaciones de control con el comando `session-vlan 4090` el ID VLAN se recomienda el más alto posible y no ser utilizado para ser VLAN de datos.
4. Creación de una VLAN independiente para la comunicación entre miembros del cluster en caso de alguna falla y su negociación entre master y backup con el comando `keep-alive-vlan "id de VLAN"` esta VLAN se configuro en modo tagged

5. Establecer todas la VLAN como miembros del cluster, cada nueva VLAN se deberá especificar en el cluster, con el comando `member-vlan "ID de VLAN"`.
6. Establecer la comunicación entre los dos miembros del MCT con los comandos `icl "nombre del cluster" ethernet "slot/port"` y `peer 1.1.1.2 rbridge-id 2 icl "nombre del cluster"` donde se especifican tanto los puertos del equipo del equipo master como la dirección IP de la vlan-seesion y rbridge-id del otro miembro.
7. Aplicar el comando `deploy` para aplicar la configuración.
8. Establecer los clientes que se encontrarán bajo la configuración del cluster, cabe mencionar que estos clientes deberán tener una configuración previa de LAG (Link Aggregaation trunk) y tener un ID idéntico en ambos equipos de cluster para lograr la comunicación entre los miembros. Los comandos utilizados son:

```
      client "nombre del cliente referente al miembro"
        rbridge-id "ID que deberá ser igual en ambos miembros"
      client-interface ethernet "slot/puerto"
deploy
```

Configuración de cluster en switches de capa 3 MLX A.

```
cluster MCT 1
 rbridge-id 1
 session-vlan 4090
 keep-alive-vlan 3
 member-vlan 2
 member-vlan 4 to 35
 member-vlan 39
 member-vlan 42 to 50
 member-vlan 52
 member-vlan 56
 member-vlan 60 to 65
 member-vlan 110 to 117
 member-vlan 120 to 123
 member-vlan 155 to 157
 member-vlan 166
 member-vlan 171 to 186
 member-vlan 198 to 199
 member-vlan 201 to 223
 member-vlan 252 to 253
```

```
 icl MCT ethernet 3/1
 peer 1.1.1.2 rbridge-id 2 icl MCT
 deploy
 client Client-P1-A
  rbridge-id 100
  client-interface ethernet 4/1
  deploy
 client Client-P2-A
  rbridge-id 200
  client-interface ethernet 4/2
  deploy
 client Client-P3-A
  rbridge-id 300
  client-interface ethernet 4/3
  deploy
 client Client-P4-A
  rbridge-id 400
  client-interface ethernet 4/4
  deploy
 client Client-P5-A
  rbridge-id 500
  client-interface ethernet 4/5
  deploy
 client Client-PB-A
  rbridge-id 700
  client-interface ethernet 4/7
  deploy
 client Client-STackPoE-A
  rbridge-id 800
  client-interface ethernet 1/2
  deploy
 client Client-Brocade624dc
  rbridge-id 900
  client-interface ethernet 1/24
deploy
```

Configuración de cluster en switches de capa 3 MLX B.

```
cluster MCT 1
 rbridge-id 2
 session-vlan 4090
 keep-alive-vlan 3
 member-vlan 2
 member-vlan 4 to 35
 member-vlan 39
 member-vlan 42 to 50
 member-vlan 52
 member-vlan 56
 member-vlan 60 to 65
 member-vlan 110 to 117
 member-vlan 120 to 123
 member-vlan 155 to 157
```

```
 member-vlan 166
 member-vlan 171 to 186
 member-vlan 198 to 199
 member-vlan 201 to 223
 member-vlan 252 to 253
 icl MCT ethernet 3/1
 peer 1.1.1.1 rbridge-id 1 icl MCT
 deploy
 client Client-P1-B
  rbridge-id 100
  client-interface ethernet 4/1
  deploy
 client Client-P2-B
  rbridge-id 200
  client-interface ethernet 4/2
  deploy
 client Client-P3-B
  rbridge-id 300
  client-interface ethernet 4/3
  deploy
 client Client-P4-B
  rbridge-id 400
  client-interface ethernet 4/4
  deploy
 client Client-P5-B
  rbridge-id 500
  client-interface ethernet 4/5
  deploy
 client Client-PB-B
  rbridge-id 700
  client-interface ethernet 4/7
  deploy
 client Client-STackPoE-B
  rbridge-id 800
  client-interface ethernet 1/2
  deploy
 client Client-Brocade624dc
  rbridge-id 900
  client-interface ethernet 1/24
deploy
```

Para que el cluster sea efectivo se necesitará aplicar el siguiente comando

```
hitless-failover enable
```

El cual es una medida de protección en caso de que la unidad master o activa falle y la unidad de backup o respaldo entre en operación sin pérdida de datos ni alarmas.

5.7 LISTA DE VLAN CREADAS (USUARIOS Y SERVIDORES)

Para la creación de VLAN fue necesaria una planeación de los segmentos de red a crear, el direccionamiento de los segmentos de red, perfiles de las VLAN y la cantidad de puertos a ocupar como se muestra en la (Tabla 12).

5.8 CREACIÓN DE LISTAS DE ACCESO

Un aspecto que se debe de considerar implementar en toda red es la seguridad entre los segmentos creados, por ello para este proyecto se crearon listas de control de acceso (ACL) de salida las cuales, restringen los accesos no autorizados de los segmentos de red de los usuarios a los segmentos de red de los servidores. En la configuración actual, el firewall es capaz de separar segmentos de red, pero debido a la ausencia de éste en los nuevos segmentos, se aplicarán listas de control de acceso para cada VLAN de servidores.

La creación de las ACL depende de un trabajo conjunto entre los administradores de las aplicaciones ya que ellos son responsables de conocer los servicios que necesitan publicar y los administradores de la red quienes administran los equipos de comunicaciones, responsables que las aplicaciones funcionen correctamente, para este proyecto se contaba con una referencia de los permisos para la red de servidores, las cuales se obtuvieron de la configuración del firewall, el cual contenía los segmentos de red de usuarios y servidores, para aplicar listas de control de acceso en la red local del instituto, se realizó la interpretación de una regla aplicada en el firewall a una ACL aplicada en los switches de capa 3.

Una configuración adicional en los switches de capa 3 para la óptima creación de ACL fue:

```
MLX_A(config)#system-max ip-filter-sys 8192
```

Comando que establece el número de sentencias en los switches de capa 3 que va desde 0 hasta 40960.

```
MLX_A(config)#enable-acl-counter
```

Muestra las estadísticas de todas las ACL, útil para verificar el número de líneas.

```
MLX_A(config)#acl-duplication-check
```

Comando utilizado para revisar las entradas duplicadas en las ACL.

La configuración de ACL está definida por dos tipos; estándar y extendida, una ACL estándar con valor numérico permitido de 1 a 99 permite o niega paquetes en base a una dirección IP origen. Una ACL extendida con valor numérico permitido de 100 a 199 permite o niega paquetes en base a protocolo IP, dirección IP origen, dirección IP destino, puerto TCP/UDP origen, puerto TCP/UDP destino.

Sintaxis para la creación de listas de acceso

ACL estándar

Syntax: [no] access-list <*num*>deny | permit <*source-ip*>| <*hostname*><*wildcard*>
or
Syntax: [no] access-list <*num*>deny | permit <*source-ip*>/<*mask-bits*>| <*hostname*>
Syntax: [no] access-list <*num*>deny | permit host <*source-ip*>| <*hostname*>
Syntax: [no] access-list <*num*>deny | permit any
Syntax: [no] ip access-group <*num*>in

ACL extendida

Syntax: [no] access-list <*num*>deny | permit <*ip-protocol*>
<*source-ip*>| <*hostname*><*wildcard*>
[<*operator*><*source-tcp/udp-port*>]
<*destination-ip*>| <*hostname*><*wildcard*>
[<*operator*><*destination-tcp/udp-port*>]
[<*icmp-type*>] [established] [precedence <*name*>| <*num*>]

[tos <*number*>] [dscp-mapping <*number*>]
[dscp-marking <*number*>] | [fragment] [non-fragment]
[option value | name | keyword] [priority <*priority-value*>| priority-force <*priority-value*>|
priority-mapping <*priority-value*>] [mirror]
Syntax: [no] access-list <*num*>deny | permit host <*ip-protocol*>any any
Syntax: [no] ip access-group <*num*>in | out

Los aspectos importantes a considerar para la creación de listas de control de acceso (ACL) para este proyecto, fué la asignación de una ACL a una interface virtual, siendo el procedimiento el siguiente:

1. Crear un script (bloc de notas) para mantener en orden las ACL aplicadas a cada una de las VLAN.
2. Ingresar a la interface virtual a la cual se implementará seguridad con el comando `interface ve "ID referente a la VLAN".`
3. Limpiar la configuración de la ACL de salida con el comando `no ip access-group "ID referente a la VLAN" out.`
4. Salir del modo configuración interface virtual con el comando `exit.`
5. Limpiar la configuración de la ACL extendida con el comando `no ip access-list extended "ID referente a la VLAN".`
6. Creación de una nueva ACL extendida con el comando `ip access-list extended "ID referente a la VLAN".`
7. Creación de todas las líneas de configuración, que restringirán o permitirán los accesos, según un análisis de permisos previo.
8. Negar todos los segmentos de red de la red LAN, permitiendo solo los mencionados en líneas superiores debido a que una ACL se aplica de manera descendente, con el comando `deny ip "redes con restricción" "mascara de redes con restricción" "red con actual ACL" "mascara de red con actual ACL".`
9. Permitir el resto del tráfico asegurando los accesos VPN a los segmentos de red local, con el comando `permit ip any any.`
10. Salir de la configuración ACL extendida con el comando `exit`
11. Volver a aplicar ACL por cambios realizados recientes, desde el modo configuración global con el comando `ip rebind-acl "ID de VLAN".`

12. Ingresar nuevamente a la interface virtual a la cual se le aplicará ACL con el comando `interface ve "ID de VLAN"`
13. Asignar la ACL de salida a la interface virtual con el comando `ip access-group ""ID de VLAN out`
14. Salir de la configuración ACL aplicada en la interface virtual, con el comando `exit`
15. Volver a aplicar ACL con el comando `ip rebind-acl "ID de VLAN".`

Estos pasos se deberán de seguir para cada ACL que se desee aplicar a alguna interface virtual. **Ver Anexo No. 4**

Por mejores prácticas se realizó un script (archivo txt) en el cual se mantendrán por separado las ACL de cada una de las VLAN y hacer las modificaciones en cada una de ellas cuando se necesite, para aplicar una ACL se debe ingresar a los switches de capa 3 por la interface de línea de comando, en modo configuración global y copiar el script para después validar su correcta instalación.

5.9 CONFIGURACIÓN DE RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto destino. Las rutas estáticas por default especifican un gateway (puerta de enlace) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce.

La configuración de las rutas estáticas en la mayoría de las marcas incluyendo la marca utilizada para este proyecto se establece con los siguientes argumentos:

```
MLX_A(config)#ip route [IP segmento destino] [máscara red destino] [IP siguiente salto]
```

La principal razón de la creación de las rutas estáticas es para el enrutamiento de tráfico que se desconoce, en una red de área local es indispensable una ruta estática para enrutar todo el tráfico que esta fuera de la red local, como DMZ y tráfico con destino a Internet, el cual contiene un gran número de segmentos de red desconocidos para la red local.

Se muestran las rutas estáticas configuradas en ambos equipos:

```
ip route 0.0.0.0/0 172.16.37.2
ip route 172.17.29.0/24 172.16.37.2
ip route 172.20.69.0/24 172.16.37.2
ip route 172.20.149.0/24 172.16.37.2
ip route 192.168.3.0/24 172.16.37.2
ip route 192.168.100.0/29 172.16.37.2
```

5.10 CONFIGURACIÓN DE LAG

Esta configuración es parte del cluster realizado entre los switches de capa 3, la creación de lag (Link Aggregation Trunk) es relevante debido a que se establecen los puertos por los cuales se transmitirá más de una VLAN, evitando los loops entre los switches de capa 3, debido a que estos puertos corresponden a la conexión hacia los diferentes stack de switches.

Creación de LAG en MLX A

```
MLX-A(config)#
lag "1" dynamic id 1
 ports ethernet 3/1 to 3/2
 primary-port 3/1
 deploy
 port-name "ICL-to-MLX-B:3/1" ethernet 3/1
 port-name "ICL-to-MLX-B:3/2" ethernet 3/2
!
lag "10" dynamic id 10
 ports ethernet 1/24
 primary-port 1/24
 deploy
 port-name "stack624dc" ethernet 1/24
!
lag "11" dynamic id 11
 ports ethernet 1/23
 primary-port 1/23
 deploy
 port-name "stack624" ethernet 1/23
!
lag "2" dynamic id 2
 ports ethernet 4/1
```

```
 primary-port 4/1
 deploy
 port-name "lag-client-SW-P1-A" ethernet 4/1
!
lag "3" dynamic id 3
 ports ethernet 4/2
 primary-port 4/2
 deploy
 port-name "lag-client-SW-P2-A" ethernet 4/2
!
lag "4" dynamic id 4
 ports ethernet 4/3
 primary-port 4/3
 deploy
 port-name "lag-client-SW-P3-A" ethernet 4/3
!
lag "5" dynamic id 5
 ports ethernet 4/4
 primary-port 4/4
 deploy
 port-name "lag-client-SW-P4-A" ethernet 4/4
!
lag "54321" dynamic id 100
 ports ethernet 1/22
 primary-port 1/22
 deploy
 port-name "LAG-BrocadeData" ethernet 1/22
!
lag "6" dynamic id 6
 ports ethernet 4/5
 primary-port 4/5
 deploy
 port-name "lag-client-SW-P5-A" ethernet 4/5
!
lag "8" dynamic id 8
 ports ethernet 4/7
 primary-port 4/7
 deploy
 port-name "lag-client-SW-PB-A" ethernet 4/7
!
lag "9" dynamic id 9
 ports ethernet 1/2
 primary-port 1/2
 deploy
 port-name "Stk624" ethernet 1/2
```

Creación de LAG en MLX B

```
MLX-B(config)#
lag "1" dynamic id 1
 ports ethernet 3/1 to 3/2
 primary-port 3/1
 deploy
 port-name "ICL-to-MLX-A:3/1" ethernet 3/1
 port-name "ICL-to-MLX-A:3/2" ethernet 3/2
!
lag "10" dynamic id 10
 ports ethernet 1/24
 primary-port 1/24
 deploy
 port-name "stack624dc" ethernet 1/24
!
lag "11" dynamic id 11
 ports ethernet 1/23
 primary-port 1/23
 deploy
 port-name "stack624" ethernet 1/23
!
lag "2" dynamic id 2
 ports ethernet 4/1
 primary-port 4/1
 deploy
 port-name "lag-client-SW-P1-B" ethernet 4/1
!
lag "3" dynamic id 3
 ports ethernet 4/2
 primary-port 4/2
 deploy
 port-name "lag-client-SW-P2-B" ethernet 4/2
!
lag "4" dynamic id 4
 ports ethernet 4/3
 primary-port 4/3
 deploy
 port-name "lag-client-SW-P3-B" ethernet 4/3
!
lag "5" dynamic id 5
 ports ethernet 4/4
 primary-port 4/4
 deploy
 port-name "lag-client-SW-P4-B" ethernet 4/4
!
lag "6" dynamic id 6
 ports ethernet 4/5
 primary-port 4/5
 deploy
 port-name "lag-client-SW-P5-B" ethernet 4/5
```

```
!
lag "8" dynamic id 8
 ports ethernet 4/7
 primary-port 4/7
 deploy
 port-name "lag-client-SW-PB-B" ethernet 4/7
!
lag "9" dynamic id 9
 ports ethernet 1/2
 primary-port 1/2
 deploy
port-name "lag-client-StackPoE-B" ethernet 1/2
```

5.11 CONFIGURACIÓN DE COMUNICACIÓN CAPA 2

Esta configuración esta deshabilitada por valores de fábrica dado que los equipos son switches de capa 3, por ello es necesario habilitar esta función para la correcta operación de la creación de las VLAN.

```
MLX-A(config)#
MLX-A(config)#no route-only
```

5.12 CONFIGURACIÓN DE STP

Este protocolo es soportado por la mayoría de los switches de diferentes marcas, la característica de este protocolo es la supresión de bucles en la red, por medio del bloqueo de algunos puertos para impedir el tráfico de enlaces redundantes y encontrar el camino más corto de un origen a un destino, la configuración de este protocolo dependerá de las necesidades de la red de cada organización. Para la marca brocade existen tres tipos de niveles:

Global: afecta a todas las VLAN del dispositivo brocade

```
Brocade(config)#spanning-tree
```

Por VLAN individual: afecta a todos los puertos que contienen la VLAN a especificar

```
Brocade(config)# vlan 10
Brocade(config-vlan-10)# spanning-tree
```

Por puerto individual: Afecta solamente a los puertos que se especifican.

```
Brocade(config)# interface 1/1
Brocade(config-if-e1000-1/1)# spanning-tree
```

Para el caso del instituto la configuración del protocolo spaning tree depende de la configuración de los servidores, en los equipos switches de capa 3 está habilitada de manera global, pero no así en las VLAN creadas.

Comandos necesarios en equipos core MLX

Existen una diversidad de comandos a utilizar en cualquier marca, para el caso del instituto los switches son de marca brocade e igual que otras marcas utilizan comando propios, algunos de ellos son necesarios para la correcta operación de la red. Para el proyecto se utilizararán los siguientes comandos en los switches de capa 3 MLX brocade.

```
Comando
fdp run
```

fdp (Foundry Discovery Protocol) comando deshabilitado por default, utilizado para alertar a dispositivos de marca brocade la existencia de otro, este aviso incluye: hostname, plataforma y capacidad del equipo, versión de software, VLAN y dirección de capa 3.

```
Comando
optical-monitor 1
```

Comando opcional cuya utilidad es el monitoreo de adaptadores de fibra óptica, este monitoreo puede ser de manera global en el equipo o por puerto y es capaz de registrar la temperatura y los niveles de energía con los cuales se encuentra operando. En una red LAN es importante el monitoreo de las interfaces teniendo especial atención a los enlaces de fibra óptica.

CAPÍTULO VI
RESULTADOS

CAPÍTULO VI. RESULTADOS

Al implementar este proyecto se consideró cambiar la arquitectura de una red plana, a una segmentada por VLAN dividiendo la red en subredes y formar estaciones de trabajo independientes según sea el caso, estos grupos de trabajo serán parte de una misma red conmutada.

La segmentación por VLAN reduce los dominios de broadcast y ayuda en la administración de la red separando segmentos lógicos de una red de área local. Con la finalidad que la información de cada estación de trabajo no se vea comprometida por usuarios no autorizados, se obtendrá una mejor administración de cada segmento de voz y de datos, manteniendo la alta disponibilidad y seguridad, todo ello sin impedir el crecimiento del personal factor muy importante dentro del concepto de escalabilidad.

Los beneficios obtenidos con la implementación de la red en base a una segmentación por VLAN son los siguientes:

- **Flexibilidad:** mayor flexibilidad en la administración y a cambios de la red, las VLAN agregan dispositivos de red y usuarios para admitir los requerimientos de cada institución.
- **Seguridad**: se podrá separar del resto de la red los grupos que tienen datos sensibles, disminuyendo las posibilidades de que ocurran accesos no permitidos a información confidencial.
- **Reducción de costos**: no es necesario implementar un router para cada segmento de red, bajo costo en la migración de red plana y el uso más eficiente de enlaces y ancho de banda existente.
- **Mejor rendimiento**: la división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red y potencia el rendimiento.

- **Mitigación de la tormenta de broadcast**: la división de una red en las VLAN reduce el número de dispositivos que pueden participar en una tormenta de broadcast.
- **Mayor eficiencia del personal de TI**: Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.

6.1 DOCUMENTACIÓN LÓGICA Y FÍSICA DE LA IMPLEMENTACIÓN DE LA RED

La documentación de toda implementación es importante y más aún la implementación de una red, por ello, es indispensable registrar cada cambio y actualización para una mejor administración facilitando cualquier información que se requiera. Crear esta documentación ayuda a corregir posibles problemas en la red.

Direccionamiento lógico (Tabla 13) y físico de la red local (Fig.49).

Direccionamiento Lógico	Mascara de Red	Tipo de Servicio
172.16.2.X - 172.16.63.X 172.20.20.X -172.20.63.X 192.168.124.0 192.168.125.0 192.168.126.0 192.168.127.0	255.255.255.0	Servidores (aplicaciones, base datos, Desarrollo)
192.168.3.X - 192.168.3.X	255.255.255.0	DMZ
192.168.5.X - 192.168.5.X	255.255.255.0	CAS
172.19.0.X - 172.19.55.X 172.19.144.X -172.19.151.X	255.255.248.0	LAN Usuarios
172.18.0.X - 172.18.7.X	255.255.248.0	LAN Voz
10.1.1.0	255.255.255.0	LAN de Administración
172.16.37.0 172.17.29.0	255.255.255.0	Segmentos de ruteo de Ruteo LAN
201.151.79.0 201.148.19.0	255.255.255.0	Segmentos de ruteo de Ruteo WAN

Tabla 13 “Direccionamiento lógico de la red local” Fuente: (creación propia, 2014).

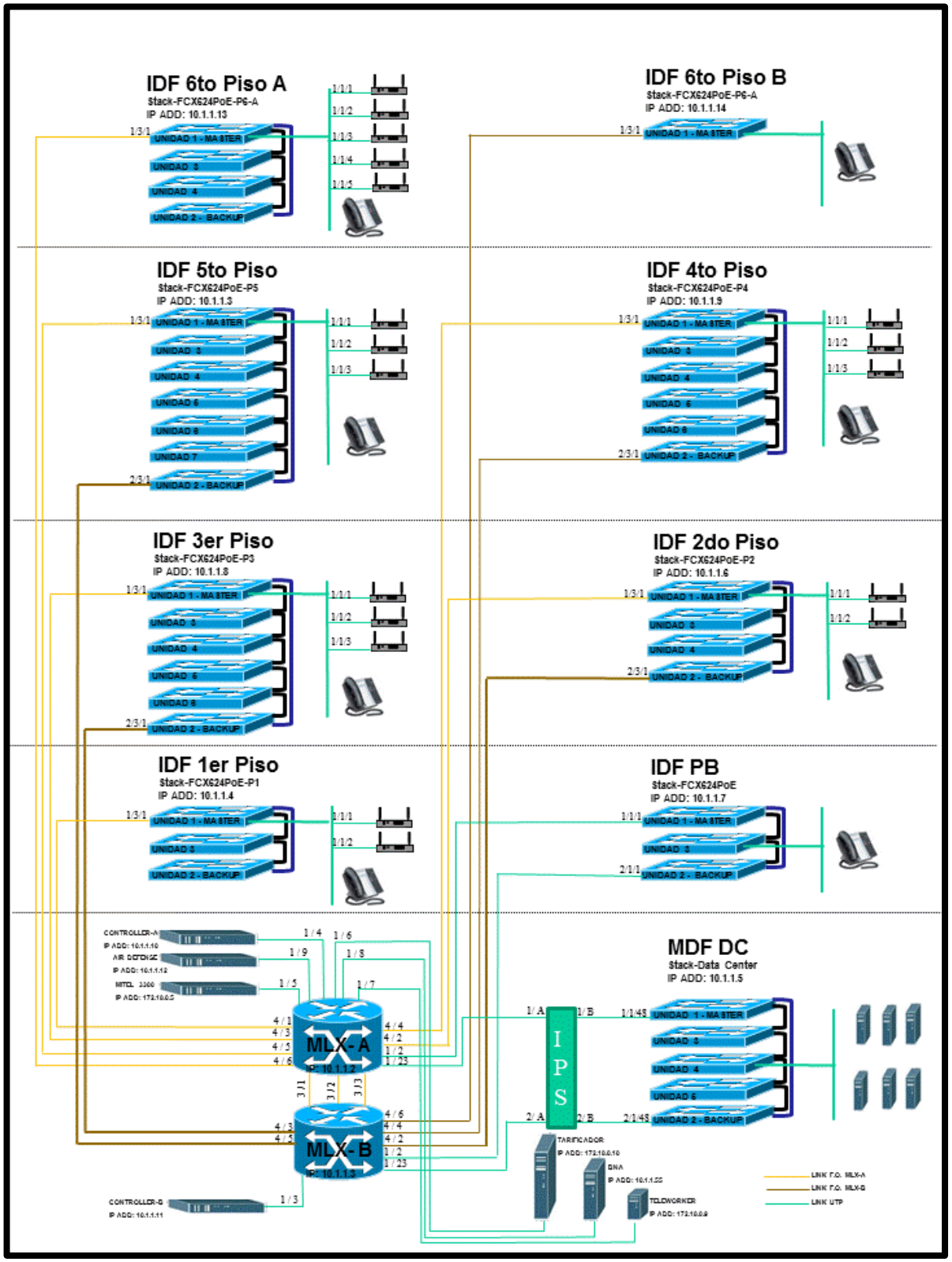

Fig. 49 “Diagrama físico de la red local” Fuente: (creación propia, 2014).

6.2 CONTRIBUCIONES Y MEJORAS

La actualización de una red local plana a una red local segura, segmentada con los servicios de voz y datos en una dependencia como el IFAI, la cual resuelve peticiones del público en general, contribuyó notablemente a los usuarios locales quienes ahora cuentan con un acceso seguro, rápido y confiable a los servicios que operan dentro de la institución, esta actualización se ve reflejada en un mejor servicio para la sociedad quien solicita información o manifiestan alguna queja sobre el derecho de sus datos personales, las mejorías realizadas se enfocan en los equipos de comunicaciones, los cuales fueron actualizados con mayor capacidad de procesamiento, que se refleja en mejores tiempos de respuesta en los servicios brindados. La utilización de la tecnología PoE para el servicio de voz sobre IP ha optimizado el cableado para los servicios de voz y datos y la implementación de la tecnología VLAN para la segmentación de los servicios proporciona; un óptimo desempeño, una mejor administración y seguridad ofreciendo así a los usuarios locales, servicios más eficientes para realizar sus actividades cotidianas, cuyo fin son resoluciones a peticiones realizadas por los ciudadanos ya sea de manera presencial o de cualquier parte del mundo con el simple hecho de tener acceso a internet y acceder a cualquier aplicación del instituto.

6.2.1 ÁREAS DE OPORTUNIDAD DE MEJORA (LIMITANTES)

El proyecto presentado tuvo como principal objetivo la actualización de una red, segmentando los servicios de voz y datos, sin embargo, en un escenario en el cual se tienen publicadas aplicaciones para el acceso público en general y se cuenta con un aumento constante de usuarios locales, es indispensable la aplicación de otras tecnologías para el óptimo funcionamiento de una red institucional, por ello se mencionarán temas que se pueden desarrollar para complementar este proyecto.

El proyecto actual como se ha mencionado solo se enfatizó en la segmentación de los servicios de voz y datos, por ello, se recomienda tener en cuenta varias aspectos que aunque no son parte de este proyecto, si son necesarios para su funcionamiento como; los enlaces troncales del servicio de voz, la instalación de un conmutador donde se centralicen todas las extensiones telefónicas, la instalación de un tarificador para recolectar registros de las llamadas realizadas.

Para el servicio de datos se recomienda desarrollar varios temas los cuales optimicen su funcionamiento como, la implementación de un servidor de DHCP tanto para la red Ethernet, como para el servicio de voz logrando facilitar la administración y asignación del direccionamiento IP, directorio activo; servicio necesario para crear usuarios y grupos con el fin de administrar inicios de sesión y actualizaciones y políticas en toda la red local, todo ello sin dejar a un lado la seguridad, por ello, se recomienda la implementación de un servicio que sea capaz de restringir y controlar accesos en la red local, solución que aparece en un servidor RADIUS tecnología recomendada por ser una de las más robustas en la implementación de una red.

6.3 RECOMENDACIONES

En cualquier red siempre se recomienda adquirir en medida de lo posible equipos más actualizados y con la mayor tecnología, sin embargo, se debe tener en cuenta aspectos básicos como la documentación de cualquier cambio o actualización, el constante mantenimiento de los equipos, etc. Teniendo en cuenta esto se recomienda:

- Dar a conocer las políticas de seguridad establecidas en la red a todos los usuarios con el fin de que sean conscientes a que servicios de la red tendrá acceso.

- Realizar la documentación de toda contingencia registrada, en este documento deberán estar descritos los pasos a seguir de cómo se dio solución parcial o completa a la falla presentada.
- Mantener un diseño flexible de la red con un crecimiento de usuarios y una mejor incorporación de nuevas tecnologías.
- Mantener en todo lo posible un diseño de la red con redundancia para garantizar la disponibilidad de los servicios
- Estar en constante estudio de las nuevas tecnologías de la información, como el caso del protocolo IPv6 y cuya mayoría de los equipos de red ya utiliza.

Este proyecto queda abierto a futuras propuestas de tesis como la implementación de DHCP, RADIUS, conmutador, tarificador, directorio activo, redes inalámbricas y nuevos y actualizados estándares.

CONCLUSIONES

Al realizar un diseño de red, no siempre se cuenta con la fortuna de desarrollarlo desde sus inicios, ya que en la mayoría de las ocasiones se cuenta con un diseño ya establecido, el cual se deberá mejorar y actualizar, tal fue el caso de este proyecto en el que ya se contaba con un previo diseño, una red plana con un solo dominio de broadcast, siendo propensa a colisiones que afectarían a toda la red y sus servicios, por ello se consideró la implementación de nuevas tecnologías que permitieran un mejor funcionamiento y administración.

Con la segmentación de los servicios de voz y datos se pretende mantener y mejorar los servicios a los usuarios internos y externos que utilizan la red del instituto IFAI. Las mejorías que se obtuvieron con la implementación de este proyecto fueron:

Mejor administración, debido a la división de redes más pequeñas en base a un grupo de trabajo, por ubicación de usuarios, etc. Facilitando la aplicación de políticas de seguridad, la comunicación entre segmentos, además de una sencilla y más rápida identificación de fallas.

Velocidad de comunicación, esta segmentación disminuye en gran medida el tráfico innecesario que se tenía con un solo dominio de broadcast ya que usuarios o servicios que anteriormente difundían mensajes de broadcast, en toda la red, ahora con esta nueva implementación se realizará sólo en su dominio de broadcast, limitada por la VLAN, permitiendo así un incremento en la velocidad de comunicación.

Disponibilidad de la red, debido a la creación de VLAN es más fácil la identificación de incidentes, problemas y conflictos en el tráfico de un dominio de

broadcast, sin que éste afecte a los demás, garantizando los servicios locales de la red.

Calidad de servicio y seguridad, con la separación de los servicios de voz y datos por medios de VLAN diferentes, es posible garantizar la disponibilidad de cada servicio independiente uno del otro y mediante la aplicación de ACL, se refuerza la seguridad de la comunicación entre los servicios y usuarios, ya sea internos o externos.

Con la implementación de estas nuevas tecnologías no solo se buscó mejorar los servicios de la red, sino también se re-diseñó el direccionamiento IP, permitiendo un mayor rango para satisfacer el crecimiento del personal en la institución. Todo lo realizado se hizo teniendo en mente un solo objetivo, mejorar los servicios de red de una institución como el IFAI, que tiene como metas el proporcionar información a la sociedad.

BIBLIOGRAFÍA

Redes de Computadoras

Cuarta Edición

Andrew S. Tanenbaum

Pearson Educación, México 2003

Interconectividad de Redes con TCP/IP

Volumen I, Tercera Edición

Douglas E. Comer

Prentice Hall. 2000

Comunicaciones y Redes de Computadoras

Sexta Edición

Williams Stallings

Prentice Hall. 2003

Metodología para el diseño de redes de área local

Alberto José Fernando Marroquín Piloña

Guatemala, 2002

Telecommunication System Engineering

Tercera Edición

Roger Freeman

Wiley-Interscience. 2004

Tecnologías y redes de transmisión de datos

Primera Edición

Enrique Herrera Pérez

LIMUSA, 2003

Brocade MLX Series and NetIron Family
Configuration Guide
Publication Number 53-1002372-02
October 6, 2011

Cisco CCENT/CCNA ICND1 100-101 Official
Cert Guide

Cisco Press
Wendell Odom
800 East 96th Street
Indianapolis, IN 46240 USA

Tecnologías de Interconectividad de Redes
Ford, Merilee Editorial Prentice
1998 Hall, México DF, México

Configuration Guide
FastIron
Supporting
Publication Number 53-1001972-01
September 28, 2010

(s.f.).
Brocade. (12 de Marzo de 2006). *Servicios y Soporte*. Recuperado el 12 de Octubre de 2013, de https://www.brocade.com/service-support/index.html
Brocade Communications Systems, Inc. (10 de Junio de 2009). *Brocade NetIron - Multi Chassis Trunking (MCT) comparable to VSS, VPC, MLT, ...*Recuperado el 17 de Diciembre de 2013, de http://community.brocade.com/t5/Ethernet-Switches-Routers/Brocade-NetIron-Multi-Chassis-Trunking-MCT-comparable-to-VSS-VPC/ta-p/2087
Brocade Communications Systems, Inc. (10 de Junio de 2009). *ServerIron ADX Switch and Router Guide*. Recuperado el 06 de Noviembre de 2013, de http://www.brocade.com/support/Product_Manuals/ServerIron_SwitchRouterGuide/VRRP.7.2.html
Brocade Communications Systems, Inc. (10 de Junio de 2009). *ServerIron ADX Switch and Router Guide*. Recuperado el 15 de Noviembre de 2013, de http://www.brocade.com/support/Product_Manuals/ServerIron_SwitchRouterGuide/VLANs.5.7.html
Cisco. (s.f.). *Cisco Networking Academy*. Recuperado el 03 de Junio de 2013, de https://www.netacad.com
Computación Aplicada al Desarrollo S.A de C.V. (s.f.). *CAD*. Recuperado el 22 de febrero de 2013, de http://www.cad.com.mx/historia_de_la_computacion.htm
Computer History Museum. (2014). *computerhistory*. Recuperado el 18 de febrero de 2013, de http://www.computerhistory.org/
Ibabe, A. I. (2008). *PaginasPersonales*. Recuperado el 28 de enero de 2013, de http://paginaspersonales.deusto.es/airibar/Ed_digital/INF/Intro/Historia.html
ieee.corporate. (19 de Julio de 2014). *IEEE 802.3 ETHERNET WORKING GROUP*. Recuperado el 10 de Febrero de 2013, de http://www.ieee802.org/3/
Mainbit S.A de C.V. (2012). *Mainbit*. Recuperado el 20 de junio de 2013, de http://www.mainbit.com.mx/cableado.pdf
raduga. (2014). *IES Torres de los Herberos*. Recuperado el 16 de junio de 2013, de http://88.12.10.114:8880/electron/franjagl/st/temas/IP.pdf
Universidad de Valencia. (2014). *Universitat do Valéncia*. Recuperado el 10 de julio de 2013, de http://www.uv.es/~hertz/hertz/Docencia/teoria/codificacion.pdf
Universidad de Valladolid. (26 de septiembre de 2014). *Grupo de Comunicaciones Ópticas*. Recuperado el 14 de noviembre de 2013, de http://nemesis.tel.uva.es/images/tCO/contenidos/tema2/tema2_1_1.htm
www.sebsauvage.net. (21 de 12 de 2009). *sebsauvage.net*. Recuperado el 3 de mayo de 2013, de http://sebsauvage.net/comprendre/tcpip/protocols.pdf

APÉNDICE

ACL: lista de control de acceso.

Aplicación: programa que realiza una función directamente para un usuario.

CSMA/CD: acceso múltiple con detección de portadora y detección de colisiones, utilizado en el protocolo 802.3.

Broadcast: paquete de datos que se envía a todos los nodos de una red.

Dispositivo: estación emisora de una trasmisión.

Estándar: definición reconocida a nivel internacional de especificaciones técnicas que asegura uniformidad en todo el mundo.

Ethernet: especificación de LAN de banda base. Las redes Ethernet usan CSMA/CD que puede trabajar a diferentes velocidades.

Host: dispositivo que comunica a través de una red.

Hub: concentrador, su función primordial es concentrar las terminales y repetir la señal que recibe a todos los puertos.

LAG: link aggregation group.

LAN: redes de datos que abarcan una área geográfica relativamente pequeña y que conectan estaciones de trabajo, terminales y otros dispositivos que se encuentran en una área geográfica limitada.

Nodo: extremo final de una conexión de red o unión común a dos o más líneas de una red.

PoE: Power over Ethernet, tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar.

Protocolo: descripción de un conjunto de normas y convenciones que rigen de qué forma los dispositivos de una red intercambian información.

Red: una red son múltiples computadoras conectadas entre ellas que utilizan un sistema de comunicaciones. El objetivo de una red es que las computadoras se comuniquen y compartan archivos.

Router: dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red.

Segmento: parte de una red de computadoras en la que todos los dispositivos se comunican utilizando el mismo medio físico.

STP: spaning tree protocol, protocolo que funciona en la capa 2 del modelo OSI y que gestiona la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes.

Switch: dispositivo de red que filtra, reenvía o inunda tramas basándose en la dirección destino de cada trama. El switch opera en la capa de enlace de datos del modelo OSI.

Tagged: etiquetado, comando para indicar que una interface permite diferentes tramas con un ID o VLAN, similar a la función trunk utilizado por varios fabricantes

TCP: protocolo de control de transmisión orientado a la conexión y que suministra transmisión confiable de datos full-duplex.

UDP: protocolo de datagramas de usuario es un protocolo simple que intercambia datos sin acuse de recibo ni garantiza la entrega.

Untagged: sin etiquetar, comando para indicar que una interface permite solamente tramas con el ID o VLAN por default

VLAN: Red de área local virtual.

VoIP: voz sobre IP, es la capacidad de llevar la voz normal estilo telefonía sobre una red basada en IP.

ANEXOS

ANEXO 1. CONFIGURACIÓN DE SWITCHES CORE (NÚCLEO COLAPSADO)

MLX A

```
vlan 2 name MCT-client-VLAN
 untagged ethe 1/3 ethe 1/8 to 1/9 ethe 1/12 to 1/13 ethe 1/24
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 200
!
vlan 5 name Int-3com
 untagged ethe 1/1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 5
!
vlan 9 name Voz
 untagged ethe 1/5 to 1/7 ethe 1/15
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 9
!
vlan 10
 untagged ethe 1/23
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1
 router-interface ve 10
!
vlan 110 name PB
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 110
!
vlan 111 name Piso_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 111
!
vlan 112 name Piso_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 112
!
vlan 113 name Piso_3
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 113
!
vlan 114 name Piso_4
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 114
!
vlan 115 name Piso_5
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 115
!
vlan 116 name Piso_6
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
```

```
router-interface ve 116
!
vlan 117 name Pruebas
tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 117
!
vlan 120 name Empleados
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 120
!
vlan 121 name Visitantes
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 121
!
vlan 122 name Sistemas
 untagged ethe 1/14
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 122
!
vlan 201 name App_1
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 201
!
vlan 202 name App_2
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 202
!
vlan 203 name App_3
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 203
!
vlan 204 name App_4
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 204
!
vlan 205 name App_5
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 205
!
vlan 206 name App_6
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 206
!
vlan 207 name App_7
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 207
!
vlan 208 name App_8
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 208
!
```

```
vlan 209 name App_9
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 209
!
vlan 210 name App_10
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 210
!
vlan 211 name App_11
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 211
!
vlan 212 name App_12
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 212
!
vlan 213 name App_13
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 213
!
vlan 214 name App_14
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 214
!
vlan 215 name App_15
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 215
!
vlan 216 name Oracle_Server_1
 untagged ethe 1/11
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 216
!
vlan 217 name Oracle_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 217
!
vlan 218 name Web_Server_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 218
!
vlan 219 name Web_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 219
!
vlan 220 name SAP_Server_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 220
!
vlan 221 name SAP_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
```

```
 router-interface ve 221
!
vlan 222 name Consoles
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 222
!
vlan 223 name RCA
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 223
```

MLX B

```
vlan 2 name MCT-client-VLAN
 untagged ethe 1/24
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 200
!
vlan 3 name Keep-VLAN
 tagged ethe 3/3
!
vlan 5 name Int-3com
 untagged ethe 1/1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 5
!
vlan 9 name Voz
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 9
!
vlan 10
 untagged ethe 1/23
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1
 router-interface ve 10
!
vlan 110 name PB
 untagged ethe 1/3
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 110
!
vlan 111 name Piso_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 111
!
vlan 112 name Piso_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 112
!
vlan 113 name Piso_3
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 113
!
```

```
vlan 114 name Piso_4
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 114
!
vlan 115 name Piso_5
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 115
!
vlan 116 name Piso_6
 untagged ethe 1/12
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
router-interface ve 116
!
vlan 117 name Pruebas
tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 117
!
vlan 120 name Empleados
 untagged ethe 1/5
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 120
!
vlan 121 name Visitantes
 untagged ethe 1/6
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 121
!
vlan 122 name Sistemas
 untagged ethe 1/7
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 122
!
vlan 155
 tagged ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 155
!
vlan 156
 tagged ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 156
!
vlan 157
 tagged ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 157
!
vlan 166
 tagged ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 166
!
vlan 201 name App_1
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 201
```

```
!
vlan 202 name App_2
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 202
!
vlan 203 name App_3
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 203
!
vlan 204 name App_4
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 204
!
vlan 205 name App_5
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 205
!
vlan 206 name App_6
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 206
!
vlan 207 name App_7
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 207
!
vlan 208 name App_8
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 208
!
vlan 209 name App_9
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 209
!
vlan 210 name App_10
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 210
!
vlan 211 name App_11
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 211
!
vlan 212 name App_12
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 212
!
vlan 213 name App_13
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 213
!
vlan 214 name App_14
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
```

```
 router-interface ve 214
!
vlan 215 name App_15
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 215
!
vlan 216 name Oracle_Server_1
 untagged ethe 1/11
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 216
!
vlan 217 name Oracle_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 217
!
vlan 218 name Web_Server_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 218
!
vlan 219 name Web_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 219
!
vlan 220 name SAP_Server_1
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 220
!
vlan 221 name SAP_Server_2
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 221
!
vlan 222 name Consoles
 tagged ethe 1/2 ethe 1/4 ethe 3/1 to 3/2 ethe 4/1 to 4/8
 router-interface ve 222
!
vlan 223 name RCA
 tagged ethe 1/2 ethe 3/1 to 3/2 ethe 4/1 to 4/8
router-interface ve 223
!
```

ANEXO 2. CONFIGURACIÓN DE VLAN PARA SWITCHES DE PISOS

Switches PB

```
vlan 2 by port
 tagged ethe 1/1/1 ethe 2/1/1
 untagged ethe 3/1/1 ethe 3/1/24
!
vlan 9 name Voz by port
 tagged ethe 1/1/1 to 1/1/24 ethe 2/1/1 to 2/1/24 ethe 3/1/5 to 3/1/10
!
vlan 110 by port
 tagged ethe 1/1/1 to 1/1/24 ethe 2/1/1 to 2/1/23 ethe 3/1/5 to 3/1/10
!
vlan 117 name Pruebas by port
 tagged ethe 1/1/1 ethe 2/1/1
!
vlan 120 name Empleados by port
 tagged ethe 1/1/1 ethe 2/1/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/1/1 ethe 2/1/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/1/1 ethe 2/1/1
!


interface ethernet 1/1/1
 link-aggregate configure key 54321
 link-aggregate active
!
interface ethernet 1/1/2
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/3
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/4
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/5
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  110
 inline power power-limit 15400
```

```
!
interface ethernet 1/1/7
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/8
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  110
```

```
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/21
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/1
 link-aggregate configure key 54321
 link-aggregate active
!
interface ethernet 2/1/2
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/8
```

```
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  110
 inline power power-limit 15400
!
```

```
interface ethernet 2/1/21
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/1
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  110
 inline power power-limit 15400
!
interface ethernet 3/1/24
 inline power power-limit 15400
```

Switches Piso 1

```
vlan 2 name Management by port
 tagged ethe 1/3/1
 untagged ethe 1/1/1 to 1/1/2
```

```
!
vlan 9 name Voz by port
 tagged ethe 1/1/3 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/23 ethe
3/1/1 to 3/1/24
 untagged ethe 2/1/24
!
vlan 111 name Piso_1 by port
 tagged ethe 1/1/3 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/23 ethe
3/1/1 to 3/1/24
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1
!
interface ethernet 1/1/1
 port-name AP2-P1-A
 inline power
!
interface ethernet 1/1/2
 port-name AP2-P1-B
 inline power
!
interface ethernet 1/1/3
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/4
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/5
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/8
```

```
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  111
 inline power power-limit 15400
!
```

```
interface ethernet 1/1/21
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 1/3/1
 port-name port-name AP3-P1-B
 link-aggregate configure singleton
 link-aggregate active
!
interface ethernet 2/1/1
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/2
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  111
```

```
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/21
```

```
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/1
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/2
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/3
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  111
 inline power power-limit 15400
!
```

```
interface ethernet 3/1/11
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/15
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/16
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  111
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  111
 inline power power-limit 15400
```

```
!
interface ethernet 3/1/24
 dual-mode  111
 disable
 inline power
```

Switches Piso 2

```
vlan 2 name Management by port
 tagged ethe 1/3/1 ethe 2/3/1
 untagged ethe 1/1/1 to 1/1/2
!
vlan 9 name Voz by port
 tagged ethe 1/1/3 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24
!
vlan 112 name Piso_2 by port
 tagged ethe 1/1/3 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24
!
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1 ethe 2/3/1
!


interface ethernet 1/1/1
 port-name AP4-P2-A
 inline power power-limit 15400
!
interface ethernet 1/1/2
 port-name AP5-P2-B
 inline power power-limit 15400
!
interface ethernet 1/1/3
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/4
 dual-mode  112
 inline power power-limit 15400
```

```
!
interface ethernet 1/1/5
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/8
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  112
```

```
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/21
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 1/3/1
 link-aggregate configure key 24680
 link-aggregate active
!
interface ethernet 2/1/1
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/2
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/5
```

```
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  112
 inline power power-limit 15400
!
```

```
interface ethernet 2/1/18
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/21
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 2/3/1
 link-aggregate configure key 24680
 link-aggregate active
!
interface ethernet 3/1/1
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/2
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/3
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  112
 inline power power-limit 15400
```

```
!
interface ethernet 3/1/6
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/11
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/15
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/16
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  112
```

```
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 3/1/24
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/1
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/2
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/3
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/4
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/5
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/6
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/7
```

```
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/8
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/9
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/10
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/11
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/12
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/13
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/14
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/15
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/16
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/17
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/18
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/19
 dual-mode  112
 inline power power-limit 15400
!
```

```
interface ethernet 4/1/20
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/21
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/22
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/23
 dual-mode  112
 inline power power-limit 15400
!
interface ethernet 4/1/24
 dual-mode  112
 inline power power-limit 15400
```

Switches Piso 3

```
vlan 2 name Management by port
 tagged ethe 1/3/1 ethe 2/3/1
 untagged ethe 1/1/1 to 1/1/3
!
vlan 9 name Voz by port
 tagged ethe 1/1/4 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24 ethe 5/1/1 to 5/1/24
ethe 6/1/1 to 6/1/23
!
vlan 113 name Piso_3 by port
 tagged ethe 1/1/4 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24 ethe 5/1/1 to 5/1/24
ethe 6/1/1 to 6/1/23
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
```

```
interface ethernet 1/1/1
 port-name AP_6-P-3-A
 inline power
!
interface ethernet 1/1/2
 port-name AP-7-P3-B
 inline power power-limit 15400
!
interface ethernet 1/1/3
 port-name AP-8-P3-C
 inline power
!
interface ethernet 1/1/4
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  113
 inline power power-limit 15400
```

```
!
interface ethernet 1/1/14
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 1/3/1
 link-aggregate configure key 13579
 link-aggregate active
!
interface ethernet 2/1/1
 dual-mode  113
```

```
 inline power power-limit 15400
!
interface ethernet 2/1/2
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/14
```

```
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 2/3/1
 link-aggregate configure key 13579
 link-aggregate active
!
interface ethernet 3/1/1
 dual-mode  113
 inline power power-limit 15400
!
```

```
interface ethernet 3/1/2
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/3
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  113
 inline power power-limit 15400
```

```
!
interface ethernet 3/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/16
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 3/1/24
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/1
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/2
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/3
 dual-mode  113
```

```
 inline power power-limit 15400
!
interface ethernet 4/1/4
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/6
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/13
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/14
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/16
```

```
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/17
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/19
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/23
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 4/1/24
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/1
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/2
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/3
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/4
 dual-mode  113
 inline power power-limit 15400
!
```

```
interface ethernet 5/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/6
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/13
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/14
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/16
 dual-mode  113
!
interface ethernet 5/1/17
 dual-mode  113
 inline power power-limit 15400
!
```

```
interface ethernet 5/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/19
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/23
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 5/1/24
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/1
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/2
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/3
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/4
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/5
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/6
 dual-mode  113
 inline power power-limit 15400
```

```
!
interface ethernet 6/1/7
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/8
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/9
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/10
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/11
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/12
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/13
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/14
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/15
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/16
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/17
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/18
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/19
 dual-mode  113
```

```
 inline power power-limit 15400
!
interface ethernet 6/1/20
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/21
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/22
 dual-mode  113
 inline power power-limit 15400
!
interface ethernet 6/1/23
 dual-mode  113
 inline power power-limit 15400
```

Switches Piso 4

```
vlan 2 name Management by port
 tagged ethe 1/3/1 ethe 2/3/1
 untagged ethe 1/1/1 to 1/1/3
!
vlan 9 name Voz by port
 tagged ethe 1/1/4 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24 ethe 5/1/1 to 5/1/24
ethe 6/1/1 to 6/1/24
!
vlan 114 name Piso_4 by port
 tagged ethe 1/1/4 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24 ethe 5/1/1 to 5/1/24
ethe 6/1/1 to 6/1/24
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1 ethe 2/3/1
!


interface ethernet 1/1/1
 port-name AP-9-P4-A
 inline power
```

```
!
interface ethernet 1/1/2
 port-name AP-10-P4-B
 inline power
!
interface ethernet 1/1/3
 port-name AP-11-P4-C
 inline power
!
interface ethernet 1/1/4
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/5
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  114
```

```
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 1/3/1
 link-aggregate configure key 12357
 link-aggregate active
!
interface ethernet 2/1/1
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/2
```

```
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  114
 inline power power-limit 15400
!
```

```
interface ethernet 2/1/15
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 2/3/1
 link-aggregate configure key 12357
 link-aggregate active
!
interface ethernet 3/1/1
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/2
 dual-mode  114
 inline power power-limit 15400
```

```
!
interface ethernet 3/1/3
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/15
 dual-mode  114
```

```
 inline power power-limit 15400
!
interface ethernet 3/1/16
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 3/1/24
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/1
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/2
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/3
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/4
```

```
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/5
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/7
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/14
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/15
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/16
 dual-mode  114
 inline power power-limit 15400
!
```

```
interface ethernet 4/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/18
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/19
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 4/1/24
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/1
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/2
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/3
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/4
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/5
 dual-mode  114
 inline power power-limit 15400
```

```
!
interface ethernet 5/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/7
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/14
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/15
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/16
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/18
 dual-mode  114
```

```
 inline power power-limit 15400
!
interface ethernet 5/1/19
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 5/1/24
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/1
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/2
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/3
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/4
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/5
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/6
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/7
```

```
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/8
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/9
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/10
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/11
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/12
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/13
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/14
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/15
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/16
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/17
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/18
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/19
 dual-mode  114
 inline power power-limit 15400
!
```

```
interface ethernet 6/1/20
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/21
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/22
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/23
 dual-mode  114
 inline power power-limit 15400
!
interface ethernet 6/1/24
 dual-mode  114
 inline power power-limit 15400
```

Switches de Piso 5

```
vlan 2 name Management by port
 tagged ethe 1/3/1 ethe 2/3/1
 untagged ethe 1/1/1 to 1/1/3 ethe 4/1/13
!
vlan 9 name Voz by port
 tagged ethe 1/1/5 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/2 ethe 4/1/4 to 4/1/12
ethe 4/1/14 to 4/1/22 ethe 4/1/24 ethe 5/1/1 to 5/1/24 ethe 6/1/1 to
6/1/24 ethe 7/1/1 to 7/1/24
!
vlan 115 name Piso_5 by port
 tagged ethe 1/1/5 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
2/3/1 ethe 3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/2 ethe 4/1/4 to 4/1/12
ethe 4/1/14 to 4/1/22 ethe 4/1/24 ethe 5/1/1 to 5/1/24 ethe 6/1/1 to
6/1/24 ethe 7/1/1 to 7/1/24
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1 ethe 2/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1 ethe 2/3/1
!
interface ethernet 1/1/1
```

```
 port-name AP-12-P5-A
 inline power
!
interface ethernet 1/1/2
 port-name AP-13-P5-B
 inline power
!
interface ethernet 1/1/3
 port-name AP-14-P5-C
 inline power power-limit 15400
!
interface ethernet 1/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  115
 inline power power-limit 15400
!
```

```
interface ethernet 1/1/15
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 1/3/1
 link-aggregate configure key 32145
 link-aggregate active
!
interface ethernet 2/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/2
 dual-mode  115
 inline power power-limit 15400
```

```
!
interface ethernet 2/1/3
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  115
```

```
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 2/3/1
 link-aggregate configure key 32145
 link-aggregate active
!
interface ethernet 3/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/2
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/3
```

```
 dual-mode  115
 speed-duplex 100-full
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/15
 dual-mode  115
 inline power power-limit 15400
```

```
!
interface ethernet 3/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 3/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/2
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/5
 dual-mode  115
```

```
 inline power power-limit 15400
!
interface ethernet 4/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/15
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/19
```

```
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 4/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/2
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/3
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/8
 dual-mode  115
 inline power power-limit 15400
!
```

```
interface ethernet 5/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/15
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/21
 dual-mode  115
 inline power power-limit 15400
```

```
!
interface ethernet 5/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/23
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 5/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/2
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/3
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/10
 dual-mode  115
```

```
 inline power power-limit 15400
!
interface ethernet 6/1/11
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/15
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/23
```

```
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 6/1/24
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/1
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/2
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/3
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/4
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/5
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/6
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/7
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/8
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/9
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/10
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/11
 dual-mode  115
 inline power power-limit 15400
!
```

```
interface ethernet 7/1/12
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/13
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/14
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/15
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/16
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/17
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/18
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/19
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/20
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/21
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/22
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/23
 dual-mode  115
 inline power power-limit 15400
!
interface ethernet 7/1/24
 dual-mode  115
 inline power power-limit 15400
```

Switches Piso 6

```
vlan 2 name Management by port
 tagged ethe 1/3/1
 untagged ethe 1/1/1 to 1/1/5
!
vlan 9 name Voz by port
 tagged ethe 1/1/6 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24
!
vlan 116 name Piso_6 by port
 tagged ethe 1/1/6 to 1/1/24 ethe 1/3/1 ethe 2/1/1 to 2/1/24 ethe
3/1/1 to 3/1/24 ethe 4/1/1 to 4/1/24
!
vlan 117 name Pruebas by port
 tagged ethe 1/3/1
!
vlan 120 name Empleados by port
 tagged ethe 1/3/1
!
vlan 121 name Visitantes by port
 tagged ethe 1/3/1
!
vlan 122 name Sistemas by port
 tagged ethe 1/3/1


interface ethernet 1/1/1
 inline power power-limit 15400
!
interface ethernet 1/1/2
 inline power power-limit 15400
!
interface ethernet 1/1/3
 inline power power-limit 15400
!
interface ethernet 1/1/4
 speed-duplex 100-full
 inline power power-limit 15400
!
interface ethernet 1/1/5
 inline power power-limit 15400
!
interface ethernet 1/1/6
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/7
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/8
```

```
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/9
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/10
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/11
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/12
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/13
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/14
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/15
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/16
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/17
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/18
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/19
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/20
 dual-mode  116
 inline power power-limit 15400
!
```

```
interface ethernet 1/1/21
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/22
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/23
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 1/1/24
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/1
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/2
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/3
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/4
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/5
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/6
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/7
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/8
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/9
 dual-mode  116
 inline power power-limit 15400
```

```
!
interface ethernet 2/1/10
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/11
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/12
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/13
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/14
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/15
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/16
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/17
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/18
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/19
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/20
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/21
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/22
 dual-mode  116
```

```
 inline power power-limit 15400
!
interface ethernet 2/1/23
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 2/1/24
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/1
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/2
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/3
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/4
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/5
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/6
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/7
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/8
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/9
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/10
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/11
```

```
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/12
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/13
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/14
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/15
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/16
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/17
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/18
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/19
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/20
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/21
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/22
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 3/1/23
 dual-mode  116
 inline power power-limit 15400
!
```

```
interface ethernet 3/1/24
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/1
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/2
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/3
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/4
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/5
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/6
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/7
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/8
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/9
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/10
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/11
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/12
 dual-mode  116
 inline power power-limit 15400
```

```
!
interface ethernet 4/1/13
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/14
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/15
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/16
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/17
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/18
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/19
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/20
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/21
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/22
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/23
 dual-mode  116
 inline power power-limit 15400
!
interface ethernet 4/1/24
 dual-mode  116
 inline power power-limit 15400
```

ANEXO 3. CONFIGURACIÓN DE PROTOCOLO VRRP

```
MLX_A(config)#router vrrp-extended
interface ve 5
ip address 172.16.37.3/24
 ip vrrp-extended vrid 5
  backup priority 255
  ip-address 172.16.37.1
  activate
!
interface ve 9
 ip address 172.18.0.2/21
 ip vrrp-extended vrid 9
  backup priority 255
  ip-address 172.18.0.1
  activate
!
interface ve 110
 ip address 172.19.0.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 110
  backup priority 255
  ip-address 172.19.0.1
  activate
!
interface ve 111
 ip address 172.19.8.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 111
  backup priority 255
  ip-address 172.19.8.1
  activate
!
interface ve 112
 ip address 172.19.16.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 112
  backup priority 255
  ip-address 172.19.16.1
  activate
!
interface ve 113
 ip address 172.19.24.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 113
  backup priority 255
  ip-address 172.19.24.1
  activate
!
interface ve 114
 ip address 172.19.32.2/21
```

```
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 114
  backup priority 255
  ip-address 172.19.32.1
  activate
!
interface ve 115
 ip address 172.19.40.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 115
  backup priority 255
  ip-address 172.19.40.1
  activate
!
interface ve 116
 ip address 172.19.48.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 116
  backup priority 255
  ip-address 172.19.48.1
  activate
!
interface ve 117
 ip address 172.19.144.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 117
  backup priority 255
  ip-address 172.19.144.1
  activate
!
interface ve 120
 ip address 172.19.112.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 120
  backup priority 255
  ip-address 172.19.112.1
  activate
!
interface ve 121
 ip address 172.19.120.2/21
 ip helper-address 172.20.52.26
 ip access-group 105 in
 ip vrrp-extended vrid 121
  backup priority 255
  ip-address 172.19.120.1
  activate
!
interface ve 122
 ip address 172.19.128.2/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 122
```

```
  backup priority 255
  ip-address 172.19.128.1
  activate
!
interface ve 200
 ip address 10.1.1.1/24
 ip vrrp-extended vrid 2
  backup priority 255
  ip-address 10.1.1.254
  activate
!
interface ve 201
 ip address 172.20.51.2/24
 ip vrrp-extended vrid 201
  backup priority 255
  ip-address 172.20.51.1
  activate
!
interface ve 202
 ip address 172.20.52.2/24
 ip vrrp-extended vrid 202
  backup priority 255
  ip-address 172.20.52.1
  activate
!
interface ve 203
 ip address 172.20.53.2/24
 ip vrrp-extended vrid 203
  backup priority 255
  ip-address 172.20.53.1
  activate
!
interface ve 204
 ip address 172.20.54.2/24
 ip vrrp-extended vrid 204
  backup priority 255
  ip-address 172.20.54.1
  activate
!
interface ve 205
 ip address 172.20.55.2/24
 ip vrrp-extended vrid 205
  backup priority 255
  ip-address 172.20.55.1
  activate
!
interface ve 206
 ip address 172.20.56.2/24
 ip vrrp-extended vrid 206
  backup priority 255
  ip-address 172.20.56.1
```

```
  activate
!
interface ve 207
 ip address 172.20.57.2/24
 ip vrrp-extended vrid 207
  backup priority 255
  ip-address 172.20.57.1
  activate
!
interface ve 208
 ip address 172.20.58.2/24
 ip vrrp-extended vrid 208
  backup priority 255
  ip-address 172.20.58.1
  activate
!
interface ve 209
 ip address 172.20.59.2/24
 ip vrrp-extended vrid 209
  backup priority 255
  ip-address 172.20.59.1
  activate
!
interface ve 210
 ip address 172.20.60.2/24
 ip vrrp-extended vrid 210
  backup priority 255
  ip-address 172.20.60.1
  activate
!
interface ve 211
 ip address 172.20.22.2/24
 ip vrrp-extended vrid 201
  backup priority 255
  ip-address 172.20.22.1
  activate
!
interface ve 212
 ip address 172.20.23.2/24
 ip vrrp-extended vrid 212
  backup priority 255
  ip-address 172.20.23.1
  activate
!
interface ve 213
 ip address 172.20.24.2/24
 ip vrrp-extended vrid 213
  backup priority 255
  ip-address 172.20.24.1
  activate
!
```

```
interface ve 214
 ip address 172.20.25.2/24
 ip vrrp-extended vrid 214
  backup priority 255
  ip-address 172.20.25.1
  activate
!
interface ve 215
 ip address 172.20.61.2/24
 ip vrrp-extended vrid 215
  backup priority 255
  ip-address 172.20.61.1
  activate
!
interface ve 216
 ip address 172.20.20.2/24
 ip vrrp-extended vrid 216
  backup priority 255
  ip-address 172.20.20.1
  activate
!
interface ve 217
 ip address 172.20.21.2/24
 ip vrrp-extended vrid 217
  backup priority 255
  ip-address 172.20.21.1
  activate
!
interface ve 218
 ip address 172.20.62.2/24
 ip vrrp-extended vrid 218
  backup priority 255
  ip-address 172.20.62.1
  activate
!
interface ve 219
 ip address 172.20.63.2/24
 ip vrrp-extended vrid 219
  backup priority 255
  ip-address 172.20.63.1
  activate
!
interface ve 220
 ip address 172.20.50.2/24
 ip vrrp-extended vrid 220
  backup priority 255
  ip-address 172.20.50.1
  activate
!
interface ve 221
 ip address 172.20.31.2/24
```

```
 ip vrrp-extended vrid 221
  backup priority 255
  ip-address 172.20.31.1
  activate
!
interface ve 222
 ip address 172.20.150.2/24
 ip vrrp-extended vrid 222
  backup priority 255
  ip-address 172.20.150.1
  activate
!
interface ve 223
 ip address 172.20.64.2/24
 ip vrrp-extended vrid 223
  backup priority 255
  ip-address 172.20.64.1
  activate
```

MLX B

```
MLX_A(config)#router vrrp-extended
interface ve 5
 ip address 172.16.37.4/24
 ip vrrp-extended vrid 5
  backup
  ip-address 172.16.37.1
  activate
!
interface ve 9
 ip address 172.18.0.3/21
 ip vrrp-extended vrid 9
  backup
  ip-address 172.18.0.1
  activate
!
interface ve 100
 ip address 1.1.1.2/24
!
interface ve 110
 ip address 172.19.0.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 110
  backup
  ip-address 172.19.0.1
  activate
!
interface ve 111
 ip address 172.19.8.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 111
  backup
```

```
  ip-address 172.19.8.1
  activate
!
interface ve 112
 ip address 172.19.16.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 112
  backup
  ip-address 172.19.16.1
  activate
!
interface ve 113
 ip address 172.19.24.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 113
  backup
  ip-address 172.19.24.1
  activate
!
interface ve 114
 ip address 172.19.32.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 114
  backup
  ip-address 172.19.32.1
  activate
!
interface ve 115
 ip address 172.19.40.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 115
  backup
  ip-address 172.19.40.1
  exit
!
interface ve 116
 ip address 172.19.48.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 116
  backup
  ip-address 172.19.48.1
  exit
!
interface ve 117
 ip address 172.19.144.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 117
  backup
  ip-address 172.19.144.1
  activate
!
```

```
interface ve 120
 ip address 172.19.112.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 120
  backup
  ip-address 172.19.112.1
  activate
!
interface ve 121
 ip address 172.19.120.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 121
  backup
  ip-address 172.19.120.1
  activate
!
interface ve 122
 ip address 172.19.128.3/21
 ip helper-address 172.20.52.26
 ip vrrp-extended vrid 122
  backup
  ip-address 172.19.128.1
  activate
!
interface ve 200
 ip address 10.1.1.2/24
 ip vrrp-extended vrid 2
  backup
  ip-address 10.1.1.254
  activate
!
interface ve 201
 ip address 172.20.51.3/24
 ip vrrp-extended vrid 201
  backup
  ip-address 172.20.51.1
  activate
!
interface ve 202
 ip address 172.20.52.3/24
 ip vrrp-extended vrid 202
  backup
  ip-address 172.20.52.1
  activate
!
interface ve 203
 ip address 172.20.53.3/24
 ip vrrp-extended vrid 203
  backup
  ip-address 172.20.53.1
  activate
```

```
!
interface ve 204
 ip address 172.20.54.3/24
 ip vrrp-extended vrid 204
  backup
  ip-address 172.20.54.1
  activate
!
interface ve 205
 ip address 172.20.55.3/24
 ip vrrp-extended vrid 205
  backup
  ip-address 172.20.55.1
  activate
!
interface ve 206
 ip address 172.20.56.3/24
 ip vrrp-extended vrid 206
  backup
  ip-address 172.20.56.1
  activate
!
interface ve 207
 ip address 172.20.57.3/24
 ip vrrp-extended vrid 207
  backup
  ip-address 172.20.57.1
  activate
!
interface ve 208
 ip address 172.20.58.3/24
 ip vrrp-extended vrid 208
  backup
  ip-address 172.20.58.1
  activate
!
interface ve 209
 ip address 172.20.59.3/24
 ip vrrp-extended vrid 209
  backup
  ip-address 172.20.59.1
  activate
!
interface ve 210
 ip address 172.20.60.3/24
 ip vrrp-extended vrid 210
  backup
  ip-address 172.20.60.1
  activate
!
interface ve 211
```

```
 ip address 172.20.22.3/24
 ip vrrp-extended vrid 201
  backup
  ip-address 172.20.22.1
  activate
!
interface ve 212
 ip address 172.20.23.3/24
 ip vrrp-extended vrid 212
  backup
  ip-address 172.20.23.1
  activate
!
interface ve 213
 ip address 172.20.24.3/24
 ip vrrp-extended vrid 213
  backup
  ip-address 172.20.24.1
  activate
!
interface ve 214
 ip address 172.20.25.3/24
 ip vrrp-extended vrid 214
  backup
  ip-address 172.20.25.1
  activate
!
interface ve 215
 ip address 172.20.61.3/24
 ip vrrp-extended vrid 215
  backup
  ip-address 172.20.61.1
  activate
!
interface ve 216
 ip address 172.20.20.3/24
 ip vrrp-extended vrid 216
  backup
  ip-address 172.20.20.1
  activate
!
interface ve 217
 ip address 172.20.21.3/24
 ip vrrp-extended vrid 217
  backup
  ip-address 172.20.21.1
  activate
!
interface ve 218
 ip address 172.20.62.3/24
 ip vrrp-extended vrid 218
```

```
  backup
  ip-address 172.20.62.1
  activate
!
interface ve 219
 ip address 172.20.63.3/24
 ip vrrp-extended vrid 219
  backup
  ip-address 172.20.63.1
  activate
!
interface ve 220
 ip address 172.20.50.3/24
 ip vrrp-extended vrid 220
  backup
  ip-address 172.20.50.1
  activate
!
interface ve 221
 ip address 172.20.31.3/24
 ip vrrp-extended vrid 221
  backup
  ip-address 172.20.31.1
  activate
!
interface ve 222
 ip address 172.20.150.3/24
 ip vrrp-extended vrid 222
  backup
  ip-address 172.20.150.1
  activate
!
interface ve 223
 ip address 172.20.64.3/24
 ip vrrp-extended vrid 223
  backup
  ip-address 172.20.64.1
  activate
```

ANEXO 4.CREACIÓN DE UNA ACL

```
!!!!!   172.20.61.0/24   !!!!!
!
interface ve 215
no  ip access-group VLAN_215 out
exit
no ip access-list extended VLAN_215
!
ip access-list extended VLAN_215


permit icmp any any
!
permit ip host 172.19.0.19 any
permit ip host 172.19.0.12 any
permit ip host 172.19.0.15 any
permit ip host 172.19.0.17 any
permit ip host 172.19.0.18 any
permit ip host 172.19.0.31 any
permit ip host 172.19.0.32 any
permit ip host 172.19.0.48 any
permit ip host 172.19.0.92 any

permit tcp host 172.19.24.120 host 172.20.61.20 eq 3389
!
permit tcp host 172.19.24.154 host 172.20.61.20 eq 3389
!
permit tcp host 172.19.128.40 host 172.20.61.20 eq 3389
!
permit tcp host 172.19.128.104 host 172.20.61.20 eq 3389
!!!!!
permit tcp host 192.168.127.41 eq 9077 host 172.20.61.20
permit tcp host 192.168.127.42 eq 9077 host 172.20.61.20
permit tcp host 192.168.127.46 eq 9077 host 172.20.61.20

permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 21
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 25
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 53
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 67
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 88
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 123
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 range 135 139
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 136
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 389
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 445
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 464
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 500
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 636
permit tcp 192.168.124.0 0.0.3.255  host 172.20.61.20 range 1024 65535

permit udp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 21
permit udp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 25
permit udp 192.168.124.0 0.0.3.255  host 172.20.61.20 eq 53
```

```
permit udp 192.168.124.0 0.0.3.255  host 172.20.61.20 range 67 65535

permit tcp host 172.20.52.21 host 172.20.61.20 eq 21
permit tcp host 172.20.52.21 host 172.20.61.20 eq 67
permit tcp host 172.20.52.21 host 172.20.61.20 eq 123
permit tcp host 172.20.52.21 host 172.20.61.20 eq 136
permit tcp host 172.20.52.21 host 172.20.61.20 eq 500
permit tcp host 172.20.52.21 host 172.20.61.20 range 1024 65535
permit udp host 172.20.52.21 host 172.20.61.20 eq 21
permit udp host 172.20.52.21 host 172.20.61.20 range 67 65535

permit tcp host 172.20.58.22 host 172.20.61.20 eq 21
permit tcp host 172.20.58.22 host 172.20.61.20 eq 67
permit tcp host 172.20.58.22 host 172.20.61.20 eq 123
permit tcp host 172.20.58.22 host 172.20.61.20 eq 136
permit tcp host 172.20.58.22 host 172.20.61.20 eq 500
permit tcp host 172.20.58.22 host 172.20.61.20 range 1024 65535
permit udp host 172.20.58.22 host 172.20.61.20 eq 21
permit udp host 172.20.58.22 host 172.20.61.20 range 67 65535

permit tcp host 172.20.58.23 host 172.20.61.20 eq 21
permit tcp host 172.20.58.23 host 172.20.61.20 eq 67
permit tcp host 172.20.58.23 host 172.20.61.20 eq 123
permit tcp host 172.20.58.23 host 172.20.61.20 eq 136
permit tcp host 172.20.58.23 host 172.20.61.20 eq 500
permit tcp host 172.20.58.23 host 172.20.61.20 range 1024 65535
permit udp host 172.20.58.23 host 172.20.61.20 eq 21
permit udp host 172.20.58.23 host 172.20.61.20 range 67 65535

permit tcp host 172.20.58.24 host 172.20.61.20 eq 21
permit tcp host 172.20.58.24 host 172.20.61.20 eq 67
permit tcp host 172.20.58.24 host 172.20.61.20 eq 123
permit tcp host 172.20.58.24 host 172.20.61.20 eq 136
permit tcp host 172.20.58.24 host 172.20.61.20 eq 500
permit tcp host 172.20.58.24 host 172.20.61.20 range 1024 65535
permit udp host 172.20.58.24 host 172.20.61.20 eq 21
permit udp host 172.20.58.24 host 172.20.61.20 range 67 65535

permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 21
permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 67
permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 123
permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 136
permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 500
permit tcp 172.16.47.24 0.0.0.7 host 172.20.61.20 range 1024 65535
permit udp 172.16.47.24 0.0.0.7 host 172.20.61.20 eq 21
permit udp 172.16.47.24 0.0.0.7 host 172.20.61.20 range 67 65535
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 21
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 67
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 123
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 136
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 500
permit tcp 172.16.47.32 0.0.0.7 host 172.20.61.20 range 1024 65535
permit udp 172.16.47.32 0.0.0.7 host 172.20.61.20 eq 21
permit udp 172.16.47.32 0.0.0.7 host 172.20.61.20 range 67 65535
```

```
!remark Politicas Active Directory

permit tcp any host 172.20.61.20 eq 25
permit tcp any host 172.20.61.20 eq 53
permit tcp any host 172.20.61.20 eq 88
permit tcp any host 172.20.61.20 range 135 139
permit tcp any host 172.20.61.20 eq 389
permit tcp any host 172.20.61.20 eq 445
permit tcp any host 172.20.61.20 eq 464
permit tcp any host 172.20.61.20 eq 636
permit tcp any host 172.20.61.20 range 3268 3269
permit tcp any host 172.20.61.20 eq 4080
permit tcp any host 172.20.61.20 eq 5722
permit tcp any host 172.20.61.20 range 49152 65535

permit udp any host 172.20.61.20 eq 25
permit udp any host 172.20.61.20 eq 53
permit udp any host 172.20.61.20 eq 88
permit udp any host 172.20.61.20 eq 135
permit udp any host 172.20.61.20 range 137 139
permit udp any host 172.20.61.20 eq 389
permit udp any host 172.20.61.20 eq 445
permit udp any host 172.20.61.20 eq 464
permit udp any host 172.20.61.20 eq 636
permit udp any host 172.20.61.20 eq 5722
permit udp any host 172.20.61.20 range 3268 3269
permit udp any host 172.20.61.20 range 49152 65535

permit ip host 10.1.1.12 host 172.20.61.20
permit ip host 10.1.1.15 host 172.20.61.20
permit ip host 10.1.1.16 host 172.20.61.20
permit ip host 10.1.1.17 host 172.20.61.20
permit ip host 10.1.1.18 host 172.20.61.20
permit ip host 10.1.1.19 host 172.20.61.20
permit ip host 10.1.1.20 host 172.20.61.20
permit ip host 10.1.1.21 host 172.20.61.20
permit ip host 10.1.1.22 host 172.20.61.20
permit ip host 10.1.1.23 host 172.20.61.20
permit ip host 10.1.1.24 host 172.20.61.20
permit tcp host 172.20.51.50  host  172.20.61.20 eq 123
permit udp host 172.20.51.50  host  172.20.61.20 eq 123
permit ip 172.20.52.0 0.0.0.255  host  172.20.61.20
permit udp 172.20.53.0 0.0.0.255  host  172.20.61.20 eq 123
permit ip host 172.20.53.21  host  172.20.61.20
permit udp 172.20.54.0 0.0.0.255  host  172.20.61.20 eq 123
permit ip host 172.20.54.21  host  172.20.61.20
permit udp 172.20.55.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.56.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.57.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.58.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.59.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.60.0 0.0.0.255  host  172.20.61.20 eq 123
```

```
permit udp 172.20.22.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.23.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.24.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.25.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.61.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.20.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.21.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.63.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.50.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.31.0 0.0.0.255  host  172.20.61.20 eq 123
permit udp 172.20.64.0 0.0.0.255  host  172.20.61.20 eq 123
permit tcp host 172.20.50.25  host  172.20.61.20 eq 123
permit udp host 172.20.50.25  host  172.20.61.20 eq 123
permit ip host 172.18.0.5 host 172.20.61.20
permit ip host 172.19.128.13 any
permit ip host 172.19.128.18 any
permit ip host 172.19.128.19 any
permit ip host 172.19.128.41 any
permit ip host 172.19.128.48 any
permit ip host 172.19.128.68 any
permit ip host 172.19.128.81 any
permit ip host 172.19.128.91 any
permit ip host 172.19.128.92 any
permit ip host 172.19.128.98 any
permit ip host 172.19.128.99 any
permit ip host 172.20.51.24 any
permit ip host 172.20.23.20 any
permit ip host 172.20.25.20 any
permit ip 172.19.112.0 0.0.7.255 host 172.20.61.20
permit ip 172.19.128.0 0.0.7.255 host 172.20.61.20

deny ip 172.19.0.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.8.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.16.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.24.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.32.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.40.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.48.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.144.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.112.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.120.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.128.0 0.0.7.255 172.20.61.0 0.0.0.255
deny ip 172.19.136.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.51.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.52.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.53.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.54.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.55.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.56.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.57.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.58.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.59.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.60.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.22.0 0.0.0.255 172.20.61.0 0.0.0.255
```

```
deny ip 172.20.23.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.24.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.25.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.61.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.20.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.21.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.62.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.63.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.50.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.31.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.150.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.64.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.151.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 172.20.160.0 0.0.0.255 172.20.61.0 0.0.0.255
deny ip 192.168.111.0 0.0.0.255 172.20.61.0 0.0.0.255

permit ip any any
!
!
!
!
exit
!
!
ip rebind-acl VLAN_215

!
!
!

interface ve 215

ip access-group VLAN_215 out

exit

ip rebind-acl VLAN_215
```

CREACIÓN DE ACL PARA LA VLAN 16

```
!!!!!   172.16.16.0/24   !!!!!
interface ve 16

no  ip access-group VLAN_16 out

exit

no ip access-list extended VLAN_16
!
ip access-list extended VLAN_16

permit icmp any any
!
```

```
!
permit tcp any host 172.16.16.5 eq 80
!
permit ip host 172.19.136.26 host 172.16.16.5
!
permit ip host 172.19.0.19 any
!
permit tcp host 172.19.136.21 host 172.16.16.6 eq 3306
permit tcp host 172.19.136.21 host 172.16.16.6 eq 3389
!
permit tcp 172.19.0.0 0.0.255.255 host 172.16.16.8 eq 80
!
permit tcp host 172.19.24.23 eq 23 host 172.16.16.8
permit tcp host 172.19.24.23 eq 80 host 172.16.16.8
permit tcp host 172.19.24.23 eq 443 host 172.16.16.8
permit tcp host 172.19.24.23 eq 1521 host 172.16.16.8
permit tcp host 172.19.24.23 range 8090 8091 host 172.16.16.8
!
permit tcp host 172.19.24.95 host 172.16.16.5 range 137 139
permit tcp host 172.19.24.95 host 172.16.16.5 eq 445
permit udp host 172.19.24.95 host 172.16.16.5 eq 139

permit tcp host 172.19.128.62 host 172.16.16.5 range 137 139
permit tcp host 172.19.128.62 host 172.16.16.5 eq 445
permit udp host 172.19.128.62 host 172.16.16.5 eq 139
!
permit ip host 172.19.0.12 any
permit ip host 172.19.0.15 any
permit ip host 172.19.0.17 any
permit ip host 172.19.0.18 any
permit ip host 172.19.0.31 any
permit ip host 172.19.0.32 any
permit ip host 172.19.0.48 any
permit ip host 172.19.0.92 any
!
permit tcp host 172.20.20.20 eq 3000 host 172.16.16.5
!
permit tcp host 172.20.32.10 eq 1433 host 172.16.16.5
permit tcp host 172.20.32.10 eq 3389 host 172.16.16.5
!
!permit ip 172.19.0.0 0.0.7.255 any
! permit tcp host 172.20.61.20 eq 21 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 25 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 53 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 67 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 88 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 123 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 range 135 139 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 136 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 389 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 445 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 464 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 500 172.16.16.0 0.0.0.255
permit tcp host 172.20.61.20 eq 636 172.16.16.0 0.0.0.255
```

```
permit tcp host 172.20.61.20 range 1024 65535 172.16.16.0 0.0.0.255

permit udp host 172.20.61.20 eq 21 172.16.16.0 0.0.0.255
permit udp host 172.20.61.20 eq 25 172.16.16.0 0.0.0.255
permit udp host 172.20.61.20 eq 53 172.16.16.0 0.0.0.255
permit udp host 172.20.61.20 range 67 65535 172.16.16.0 0.0.0.255
!
permit tcp 192.168.5.0 0.0.0.255 host 172.16.16.8 eq 80
!
permit tcp host 172.19.24.37 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.107 host 172.16.16.8 eq 3389
!
permit tcp host 172.19.128.107 host 172.16.16.6 eq 3089
permit tcp host 172.19.24.37 host 172.16.16.8 eq 80
permit tcp host 172.19.128.107 host 172.16.16.8 eq 80
permit tcp host 172.19.24.37 host 172.16.16.8 eq 3089
permit tcp host 172.19.128.107 host 172.16.16.8 eq 3089
!
permit tcp host 172.19.24.24 host 172.16.16.8 eq 80
permit tcp host 172.19.24.61 host 172.16.16.8 eq 80
permit tcp host 172.19.24.63 host 172.16.16.8 eq 80

permit tcp host 172.19.128.22 host 172.16.16.8 eq 80
permit tcp host 172.19.128.28 host 172.16.16.8 eq 80
permit tcp host 172.19.128.30 host 172.16.16.8 eq 80
permit tcp host 172.19.128.50 host 172.16.16.8 eq 80
permit tcp host 172.19.128.55 host 172.16.16.8 eq 80
permit tcp host 172.19.128.57 host 172.16.16.8 eq 80
permit tcp host 172.19.128.66 host 172.16.16.8 eq 80
permit tcp host 172.19.128.89 host 172.16.16.8 eq 80
permit tcp host 172.19.128.95 host 172.16.16.8 eq 80
permit tcp host 172.19.128.116 host 172.16.16.8 eq 80
permit tcp host 172.19.128.118 host 172.16.16.8 eq 80
permit tcp host 172.20.32.12 eq 4500 host 172.16.16.8
!
permit tcp host 172.19.24.63 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.95 host 172.16.16.8 eq 3389
!
permit tcp host 172.19.128.118 host 172.16.16.8 eq 3389
!
permit tcp host 172.19.24.24 host 172.16.16.8 eq 3380
permit tcp host 172.19.24.61 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.22 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.28 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.30 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.50 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.55 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.57 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.66 host 172.16.16.8 eq 3380
permit tcp host 172.19.128.89 host 172.16.16.8 eq 3380

permit tcp host 172.19.24.24 host 172.16.16.8 eq 3389
permit tcp host 172.19.24.61 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.22 host 172.16.16.8 eq 3389
```

```
permit tcp host 172.19.128.28 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.30 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.50 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.55 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.57 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.66 host 172.16.16.8 eq 3389
permit tcp host 172.19.128.89 host 172.16.16.8 eq 3389
!
permit tcp host 172.19.128.118 host 172.16.16.6 eq 3389
! permit tcp host 172.19.128.42 host 172.16.16.5 eq 3389
permit tcp host 172.19.128.42 host 172.16.16.5 range 137 139
permit tcp host 172.19.128.42 host 172.16.16.5 eq 445
permit udp host 172.19.128.42 host 172.16.16.5 eq 139
!
permit ip host 172.20.25.20 any
!
permit ip host 172.19.128.98 any
!
permit ip host 172.19.128.13 any
permit ip host 172.19.128.18 any
permit ip host 172.19.128.19 any
permit ip host 172.19.128.41 any
permit ip host 172.19.128.48 any
permit ip host 172.19.128.68 any
permit ip host 172.19.128.81 any
permit ip host 172.19.128.91 any
permit ip host 172.19.128.92 any
permit ip host 172.19.128.99 any
permit ip host 172.20.51.24 any
permit ip host 172.20.23.20 any

permit ip 172.20.64.0 0.0.0.255 172.16.16.0 0.0.0.255

permit tcp any host 172.16.16.2 eq 8088
permit tcp any host 172.16.16.2 eq 80
permit tcp any host 172.16.16.3 eq 80
permit tcp any host 172.16.16.6 eq 80
permit tcp any host 172.16.16.6 eq 443
permit tcp any host 172.16.16.7 eq 80
!
!
permit ip host 172.20.20.20 host 172.16.16.3
!
!
permit tcp host 172.19.24.61 host 172.16.16.3 eq 3389
permit tcp host 172.19.24.61 host 172.16.16.3 eq 1433

permit tcp host 172.19.128.30 host 172.16.16.3 eq 3389
permit tcp host 172.19.128.30 host 172.16.16.3 eq 1433

permit tcp host 172.19.128.50 host 172.16.16.3 eq 3389
permit tcp host 172.19.128.50 host 172.16.16.3 eq 1433

permit tcp host 172.19.128.55 host 172.16.16.3 eq 3389
```

```
permit tcp host 172.19.128.55 host 172.16.16.3 eq 1433

permit tcp host 172.19.128.57 host 172.16.16.3 eq 3389
permit tcp host 172.19.128.57 host 172.16.16.3 eq 1433

permit tcp host  172.19.24.24 host 172.16.16.3 eq 3389
permit tcp host  172.19.24.24 host 172.16.16.3 eq 1433

permit tcp host  172.19.128.28 host 172.16.16.3 eq 3389
permit tcp host  172.19.128.28 host 172.16.16.3 eq 1433
permit tcp host  172.19.128.22 host 172.16.16.3 eq 3389
permit tcp host  172.19.128.22 host 172.16.16.3 eq 1433

permit tcp host 172.19.128.50 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.50 host 172.16.16.6 eq 3306

permit tcp host 172.19.128.55 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.55 host 172.16.16.6 eq 3306

permit tcp host  172.19.24.24 host 172.16.16.6 eq 3389
permit tcp host  172.19.24.24 host 172.16.16.6 eq 3306

permit tcp host  172.19.128.28 host 172.16.16.6 eq 3389
permit tcp host  172.19.128.28 host 172.16.16.6 eq 3306

permit tcp host 172.19.128.22 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.22 host 172.16.16.6 eq 3306

permit tcp host 172.19.128.30 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.30 host 172.16.16.6 eq 3306
permit tcp host 172.19.128.51 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.51 host 172.16.16.6 eq 3306

permit tcp host 172.19.128.57 host 172.16.16.6 eq 3389
permit tcp host 172.19.128.57 host 172.16.16.6 eq 3306
permit tcp host 172.19.24.61 host 172.16.16.6 eq 3389
permit tcp host 172.19.24.61 host 172.16.16.6 eq 3306
!
!
permit tcp host 172.20.23.20 172.16.16.0 0.0.0.255 eq 2638
permit tcp host 172.20.23.20 172.16.16.0 0.0.0.255 range 7937 9936
permit udp host 172.20.23.20 172.16.16.0 0.0.0.255 eq 2638
permit udp host 172.20.23.20 172.16.16.0 0.0.0.255 range 7937 9936

permit tcp host 172.20.20.20 host 172.16.16.8 eq 80

deny ip 172.19.0.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.8.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.16.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.24.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.32.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.40.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.48.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.144.0 0.0.7.255 172.16.16.0 0.0.0.255
```

```
deny ip 172.19.112.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.120.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.128.0 0.0.7.255 172.16.16.0 0.0.0.255
deny ip 172.19.136.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.51.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.52.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.53.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.54.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.55.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.56.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.57.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.58.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.59.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.60.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.22.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.23.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.24.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.25.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.61.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.20.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.21.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.62.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.63.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.50.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.31.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.150.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.151.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 172.20.160.0 0.0.0.255 172.16.16.0 0.0.0.255
deny ip 192.168.111.0 0.0.0.255 172.16.16.0 0.0.0.255
permit ip any any
!
!
exit
!
ip rebind-acl VLAN_16
!
interface ve 16
ip access-group VLAN_16 out
exit
ip rebind-acl VLAN_16
!
```